NOTE

This Microfiche meets the quality requirements of the American National Standard for Microfiche of Documents (ANSI PH5.9-1975). However, because of imperfections in the document from which it was made, it contains images that are illegible or difficult to read. The source document for this microfiche is the best copy that could be obtained prior to filming.

CIS

Congressional Information Service, Inc
Washington, D.C.

Office of Technology Assessment

Congressional Board of the 100th Congress

MORRIS K. UDALL, *Arizona, Chairman*

TED STEVENS, *Alaska, Vice Chairman*

Senate

ORRIN G. HATCH
Utah

CHARLES E. GRASSLEY
Iowa

EDWARD M. KENNEDY
Massachusetts

ERNEST F. HOLLINGS
South Carolina

CLAIBORNE PELL
Rhode Island

House

GEORGE E. BROWN, JR.
California

JOHN D. DINGELL
Michigan

CLARENCE E. MILLER
Ohio

DON SUNDQUIST
Tennessee

AMO HOUGHTON
New York

JOHN H. GIBBONS
(Nonvoting)

Advisory Council

WILLIAM J. PERRY, *Chairman*
H&Q Technology Partners

DAVID S. POTTER, *Vice Chairman*
General Motors Corp. (Ret.)

EARL BEISTLINE
Consultant

CHARLES A. BOWSHER
General Accounting Office

CLAIRE T. DEDRICK
California Land Commission

S. DAVID FREEMAN
Lower Colorado River Authority

MICHEL T. HALBOUTY
Michel T. Halbouty Energy Co.

CARL N. HODGES
University of Arizona

RACHEL McCULLOCH
Brandeis University

CHASE N. PETERSON
University of Utah

JOSEPH E. ROSS
Congressional Research Service

Director

JOHN H. GIBBONS

The Technology Assessment Board approves the release of this report. The views expressed in this report are not necessarily those of the Board, OTA Advisory Council, or individual members thereof.

Defending Secrets, Sharing Data

New Locks and Keys for Electronic Information

CONGRESS OF THE UNITED STATES   OFFICE OF TECHNOLOGY ASSESSMENT

J952-61

Recommended Citation:

U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987).

Library of Congress Catalog Card Number 87-619856

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC 20402-9325
(order form can be found in the back of this report)

Foreword

Government agencies, private sector organizations, and individual citizens are increasingly using sophisticated communications and computer technology to store, process, and transmit valuable information. The need to protect the confidentiality and integrity of such data has become vital. This report examines Federal policies directed at protecting information, particularly in electronic communications systems.

Controversy has been growing over the appropriate role of the government in serving private sector needs for standards development and, particularly, over the appropriate balance of responsibilities between defense/intelligence agencies and civilian agencies in carrying out this role. In defining these roles and striking an appropriate balance, both private sector needs, rights, and responsibilities, on one hand, and national security interests, on the other hand, need to be carefully considered.

This report examines the vulnerability of communications and computer systems, and the trends in technology for safeguarding information in these systems. It reviews the primary activities and motivations of stakeholders such as banks, government agencies, vendors, and standards developers to generate and use safeguards. It focuses on issues stemming from possible conflicts among Federal policy goals and addresses important trends taking place in the private sector.

OTA prepared the report at the request of the House Committee on Government Operations and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary. It is the second component of OTA's assessment of new communications technologies. The first component, *The Electronic Supervisor: New Technologies, New Tensions*, was published in September, 1987.

In preparing this report, OTA drew upon studies conducted by OTA project staff, contractor reports and consultants, a technical workshop, interviews with Federal and private sector representatives, and those involved in research, manufacturing, financial services, consulting, and technical standards development. Drafts of this report were reviewed by the OTA advisory panel, officials of the National Security Agency and the Department of Defense, the National Bureau of Standards, the General Services Administration, the Department of the Treasury, and other government agencies, and by interested individuals in standards setting organizations, trade associations, and professional and technical associations.

OTA appreciates the participation and contributions of these and many other experts. The report itself, however, is solely the responsibility of OTA.

John H. Gibbons

JOHN H. GIBBONS
Director

Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information Advisory Panel

Granger Morgan, *Chairman*
Carnegie Mellon University

Peter Arment
Division of Telecommunications
State of New York

Robert R. Belair
Kirkpatrick & Lockhart

Jerry J. Berman
Chief Legislative Counsel
American Civil Liberties Union

H.W. William Caming
Consultant

Robert H. Courtney, Jr.
President
RCI

Harry B. DeMaio*
Director, Data Security Program
IBM Corp.

John Harris
Special Assistant to the President
American Federation of Government Employees (AFL-CIO)

James M. Kasson
Vice President
Rolm Corp.

Steven Lipner
Digital Equipment Corp.

Gary T. Marx
Professor of Sociology
Massachusetts Institute of Technology

Robert Morris**
Chief Scientist
National Computer Security Center
National Security Agency

Susan L. Quinones
Condello, Ryan, Piscitelli

Virginia du Rivage
Research Director
9 to 5 National Association of Working Women

Forrest Smoker
Director
Corporate Telecommunications
North American Phillips Corp.

Willis H. Ware
Corporate Research Staff
The Rand Corp.

Lawrence Wills
Director, Data Security Program
IBM Corp.

Fred H. Wynbrandt
Assistant Director
Criminal Identification and Information Branch
State of California

---

*Retired. Replaced by Lawrence Wills.

**Ex-officio.

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the advisory panel members. The panel does not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

OTA Project Staff
Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information

John Andelin, *Assistant Director, OTA*
Science, Information, and Natural Resources Division

Fred W. Weingarten, *Program Manager*
Communication and Information Technologies Program

Project Staff

Charles K. Wilk, *Project Director*
Karen G. Bandy, *Analyst*
Jim Dray, *Research Analyst*
Robert Kost, *Analyst*
Mary Ann Madison, *Analyst*
Joan Winston, *Analyst*
Michael McConathy, *Intern*
Paul Phelps, *Editor*
Jeffrey P. Cohn, *Editor*

Administrative Staff

Elizabeth A. Emanuel, *Administrative Assistant*
Audrey D. Newman, *Administrative Secretary*
Sandra Holland, *Secretary*
Rebecca A. Battle, *Secretary*

Contents

Page

Chapter 1. Executive Summary 3

Chapter 2. Introduction 13

Chapter 3. The Vulnerabilities of Electronic Information Systems 23

Chapter 4. Security Safeguards and Practices 51

Chapter 5. Improving Information Security 95

Chapter 6. Major Trends in Policy Development 131

Chapter 7. Federal Policy Issues and Options 151

Appendix A. Requesting Letters 163

Appendix B. National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems 165

Appendix C. The Data Encryption Standard 168

Appendix D. Message Authentication, Public-Key Ciphers, and Digital Signatures 174

Appendix E. Acronyms 182

Appendix F. Contributors and Reviewers 183

Chapter 1

Executive Summary

CONTENTS

Page

The Need for Information Security 4
  Safeguard Technology 5
  Users' Needs and Actions 6
The Role of the Federal Government 7
Policy Alternatives 9

Chapter 1

Executive Summary

As society becomes more dependent on computer and communications systems for the conduct of business, government, and personal affairs, it becomes more reliant on the confidentiality and integrity of the information these systems process. Information security has become especially important for applications where accuracy, authentication, or secrecy are essential.

Today's needs for information security are part of a centuries' long continuum that shifts in emphasis with changing technology and societal values. Modern electronic information systems are expanding the need for both familiar and new forms of information security.

Today's needs for information security are a part of a centuries' long continuum.

Developing adequate information security technology is a challenging task. This task is further complicated since some of these evolving needs can only be satisfied with technology that must itself be kept secret, according to Department of Defense sources, because revealing it could be damaging to U.S. intelligence operations.[1] This situation raises the practical question of whether safeguards designed for use by defense and intelligence agencies can meet the needs of commercial users without jeopardizing U.S. intelligence objectives, i.e., whether the National Security Agency (NSA) can reconcile its traditional secret posture with the openness needed to solve nondefense problems. It also raises the broader issues of the appropriate role of defense and intelligence agencies in civilian matters, and how openness and free market forces can coexist with secret operations and controls on sensitive information.

Policy for information security, long dominated by national security concerns, is now being reexamined because of its broadening effects on nondefense interests. At the center of the current controversy is the appropriate role of the Federal Government in information security. The immediate policy questions focus on whether NSA, primarily an intelligence agency, or the National Bureau of Standards (NBS), a civilian agency, should be responsible for developing information security for nondefense applications. A fundamental issue is how to resolve conflicts involving the boundary between the authority of the legislative and executive branches to make policy when national security is a consideration; a topic with implications extending well beyond the narrow confines of information security policy.

A separate, but related dimension to policymaking involves recent efforts to provide additional Government controls on unclassified information in computer databases, some Federal, some commercial. Proponents of greater Government controls argue that these databases make information so readily available to foreign governments, competitors, and those having criminal intent, that uncontrolled access to them is a threat to national security.

Congress is responding to these issues by examining alternative Federal roles in information security. Each of the three basic options for providing leadership—through NSA, NBS, or greater reliance on the private sector—has its own particular drawbacks and none is likely to completely satisfy all national objectives.

There are a number of national interests to be accommodated by policymakers. An optimum outcome would maximize the ability of free market forces to develop and apply technology to meet users' diverse and unfolding needs for information safeguards, while avoiding unnecessary restrictions on trade, innovation, and the free flow of information as well as compromises to the Nation's security.

---

[1] The terms intelligence and intelligence operations are used throughout this assessment to refer to signals intelligence.

THE NEED FOR INFORMATION SECURITY

The need for information security has existed for thousands of years, but the advent of electronic information systems—telegraph and telephone, sound and image recording, and computers and databases—has reemphasized the need for traditional safeguards and created a need for new ones. Early concerns tended to focus on controlling access to information and protecting its confidentiality.

Modern computer and communications systems are being used in ways that often require those using them to authenticate the accuracy of data, verify the identity of senders and receivers, reconstruct the details of transactions, and control access to sensitive or private data. As the use of these systems increases, the vulnerabilities, threats, and risks of misuse have become clearer, and information security has become a prominent issue for many Government agencies and private users.

Electronic information systems—telegraph and telephone, sound and image recording, computers and databases—reemphasize the need for traditional safeguards and create needs for new ones.

The computer and communications technologies on which these information systems are built, however, were not developed originally with information security in mind. They were designed for efficient and reliable service in the presence of accidental error, rather than intentional misuse, and little attention was given to protecting confidentiality. As one result, the public communications network has always been vulnerable to exploitation by those with appropriate resources (see below).

Technology can increase or decrease the vulnerability of communications to misuse. Microwave radio and cellular telephones have both increased vulnerability; optical fibers have decreased it. Still greater changes may be ahead as digital communications come into wider use.

Information security was not a key factor in the design of most computer and communications systems. As a result, some forms of unauthorized access, such as wiretaps, intercepting mobile telephone conversations, or logging into computers with easily guessed passwords, can be achieved with limited resources.

Increases in computing power and decentralization of computing functions have increased the vulnerability of computer and communications systems to unauthorized use. Two types of misuse should be distinguished: misuse by those not authorized to use or access systems and misuse by authorized users. For many public and private organizations, the latter problem is of greater concern.

The level of effort, expense, and technical sophistication needed to gain unauthorized access to computer or communications systems, even when the system being attacked employs no special safeguards, can vary widely. Some forms of covert access, such as wiretaps, intercepting mobile telephone conversations, or logging into computers with easily guessed passwords, can be achieved with very limited resources. Others, such as those intended for targeted and consistently successful unauthorized access, can require greater resources due to inherent barriers in the design of these systems. Systems protected by appropriate safeguards can deny access even to dedicated foreign intelligence agencies.

Users of computer and communications systems have widely different perceptions of the threats against which protection is needed.

Some users protect their systems only against unintentional error or amateur computer hackers. Others guard against misuse by their own employees, outsiders, or the sophisticated intelligence agencies of foreign countries.

Many businesses are concerned with the integrity of certain of their computer information, but not greatly concerned with threats to the confidentiality of their domestic communications.

There are few publicized cases of communications interception and most of these deal with the interception of government communications by foreign intelligence agencies. Not surprisingly, most commercial and private users, under ordinary circumstances, are not greatly concerned about their communications, particularly within the United States, being intercepted by foreign governments or others. Indeed, many businesses are concerned primarily with the integrity of certain of their business information and, in other cases, with the confidentiality of their sensitive information.

Early computer systems were designed to be used by trained operators in reasonably controlled work environments; therefore, only local access to the systems was of concern. Today's systems, in contrast, are often designed to be used by, almost literally, anyone from anywhere. With this ease of access to computers, new problems have emerged, both from hackers and other unauthorized users, and from employees authorized to use the systems. Available data suggest that the damage done by computer hackers to poorly safeguarded systems is less severe than originally thought, and that actual and potential misuse from employees who are authorized to use the systems is far more significant.

On the other hand, NSA is concerned with foreign intelligence gathering, a concern that has motivated it to launch programs to improve the security of nondefense computer and communications systems.

Thus, even though virtually all users have concern for some combination of confidentiality, integrity, and continuity of service, the business community and the Government agencies that deal with it often have a very different outlook and need than defense and intelligence agencies when it comes to safeguarding information in computer and communications systems. This difference is one reason why some of the business community has been reluctant to accept safeguard technologies based on NSA's assessment of needs or that are tightly controlled by NSA.

Safeguard Technology

Important techniques are emerging to improve the security of information in these systems including technical means to verify the identities of the senders of messages, authenticate their accuracy, and ensure confidentiality.

The private sector is developing a number of ways to safeguard information in computer and communications systems. These include technologies to encrypt data to make it confidential and to control access to computer systems (such as with personal identification techniques), as well as to audit system activity and other administrative procedures. In many cases, commercial safeguards for these systems are still evolving, as are users' understanding of their needs for them.

The use of information safeguards, properly applied, can vastly increase the level of resources required for potential adversaries to successfully gain access to protected systems. Some safeguards require two or more people,

Innovation is especially important for the evolution of new applications of information security.

often trusted employees, to collude in order to gain unauthorized access, while others leave audit trails to identify how the system was misused and by whom. But technical safeguards alone cannot protect information systems completely; effective management policies and administrative procedures are also needed.

Safeguard products are based both on adaptations of existing technology and on innovations. Some of the approaches to controlling access, for example, rely on the use of passwords or hand-geometry measurements. Techniques for authenticating messages include those that make use of newly developed mathematical techniques called public-key cryptography and electronic procedures for providing "digital signatures" to verify the identity of the sender of a message.

As is already becoming clear with cryptography, innovation is especially important for the evolution of new applications of information security. The capabilities now evolving will allow advances in the way many electronic transactions take place, from digital signatures and legally enforceable electronic contracts to improved individual and corporate accountability and assured confidentiality of transactions. The potential of cryptography and related mathematical techniques for transforming the ways in which automated transactions are accomplished has only begun to be explored for applications in finance, commerce, law, and government.

Some new safeguard techniques have only begun to be explored, but show promise for broad applications in commerce and society.

Users' Needs and Actions

Commercial and other users want greater information security to reduce fraud, embezzlement, and errors; cut the costs of operations; and protect proprietary and private data. Users have begun to incorporate information safeguards in a gradually expanding range of applications. For example, information security is being applied in the banking industry to reduce errors and opportunities for fraud, and in other industries as part of an increasing reliance on electronic, rather than paper-based, transactions. These electronic transactions allow businesses to simplify paper work and reduce inventory costs.

Although there are significant differences in the needs for information security even among users within the same industry, civilian users often focus on data integrity. They also tend to be especially sensitive to the importance of the ease of use and cost-effectiveness of safeguards. Many defense needs, too, resemble those of civilian users, but in addition, some defense functions, especially intelligence activities, have a primary need for confidentiality. These latter needs must be ensured, even if they entail higher cost or lowered ease of use.

Business users have tended to consolidate their requirements for common information safeguards through voluntary participation in the activities of U.S. and international organizations that develop open public standards. In contrast, NSA sets its own standards in a process that is sometimes open to the public (as is typical for computer security) and sometimes not (as is typical for communications security). These and other differences raise the question of whether information safeguards designed by and for the defense and intelligence agencies are well suited to the needs of commercial and other users.

THE ROLE OF THE FEDERAL GOVERNMENT

The Federal Government has played an active role in the development of information safeguards. NSA was established to unify U.S. signals intelligence operations against foreign communications and to protect U.S. military, intelligence, and diplomatic communications against foreign government intelligence gathering efforts. As NSA's concerns expanded to include computer security, the agency has begun to provide technological leadership for civilian uses of information safeguards, presumably in ways that minimize the impact on its foreign intelligence operations.

Federal policy for information security has long been dominated by national security interests and controlled by DoD and NSA.

In addition, the National Bureau of Standards has played a central role in setting information security standards for civilian Government agencies and certifying commercial products. NBS's role stems from the Brooks Act of 1965, which authorized it to set standards for computers used by Government agencies.

A civilian agency, NBS, has become active in the development of computer security standards since the mid-1970s. Recent policy directives, however, have shifted control back to DoD and NSA, raising questions of the boundary between civilian and military authorities.

NBS, with the active technical support of NSA, spearheaded the development of a national standard for cryptography, the Data Encryption Standard (DES). DES, which was adopted by NBS in 1977, has become the basis for many private cryptographic standards. It is also the standard in use by other civilian Government agencies. In addition, both NBS and NSA have facilitated the entry of cryptographic-based safeguards into the market by certifying and endorsing commercial products and developing guidelines for their use.

Its activities in providing standards and specifications, certifying equipment, and developing secret cryptographic algorithms, have made the Government influential in the decisions of some industries about their use of information safeguards.

In the mid-1980s, however, changing Government policies provided new direction for the Federal role in, and leadership for, information security. National Security Decision Directive 145 (NSDD-145), issued in 1984, expanded Federal concerns to include "safeguarding systems which process or communicate sensitive information from hostile exploitation," established a high-level interagency group to implement the new policy, and assigned key responsibilities to the Department of Defense and NSA.

One result of NSDD-145 was to authorize NSA to develop information safeguards for Government agencies to protect unclassified information. In effect, this meant that responsibility for certifying DES as a national standard and other safeguard technologies was transferred from NBS to NSA. In a major shift in policy, NSA announced in 1986 that it would no longer certify DES-based products for Gov-

There has been controversy about DoD restrictions on the export of cryptographic equipment embodying classified technology.

There are significant differences in users' needs for information security even among users within the same industry, which raises the question of whether information safeguards designed by and for defense and intelligence agencies are well suited to the needs of commercial and other users.

ernment use beginning in 1988. Instead, NSA said it will supply its own, secret cryptographic designs for use by U.S. companies and civilian Government agencies—a move that has raised some industry concerns because it might result in restrictions on the use of equipment embodying these designs and it might also allow NSA itself to eavesdrop on corporate communications.

This shift of responsibilities from NBS to NSA raised several other questions. One involves the efficacy of NSA-developed standards and guidelines for users outside the national security community. Another question concerns the scope of NSA's activities in light of NBS's legislated responsibilities under the Brooks Act.

In a later directive[2] intended to implement NSDD-145, the National Security Council placed new controls on what it called unclassified, but sensitive information in various Government information systems and commercial databases. These efforts raised such a protest from scientific and civil liberties organizations and the business community that the directive was rescinded during the course of congressional hearings in 1987 and NSDD-145 itself was put under review.

In the current reexamination of policy on information security, the immediate policy question is whether NSA or NBS should be responsible for nondefense applications.

The expanding sphere of national security concerns embedded in information security policy is now seen as competing with other national interests and affecting basic principles such as the appropriate balance between defense and civilian authority and public access to information.

These changes in Federal policies on information security indicate an expanding sphere of "national security" concerns—a concept whose definition is subject to interpretation and change. The changes point out clearly that Federal policy for information security, until recently a topic of little concern beyond the Government's defense and intelligence communities, now has significant impact on much broader areas of national interest, including commerce, innovation, free flow of information, and civil liberties. They also indicate that tensions are likely to recur as the use of automated information systems continues to expand.

Longstanding fundamental issues include how to resolve conflicts involving the boundary between the authority of the legislative and executive branches when national security is a consideration and the process by which these policies are developed.

---

[2] National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, National Security Council, Oct. 29, 1986.

POLICY ALTERNATIVES

Federal policy for the security of information in computer and communications systems seeks to achieve a number of objectives ranging from protecting national security to fostering development of private sector competence to meet its own needs. Policy might also seek to establish a structure within the Government that can provide leadership and standards both for defense and intelligence purposes and for the business community. Although there are often strong differences of opinion on the merits of specific Federal policies, there seems to be broad agreement on the types of goals that such policies might aim to achieve. Some of these goals are to:

- foster the ability of the private sector to meet the evolving needs of businesses and civilian agencies for information safeguards;
- minimize risks to intelligence capabilities resulting from independent, private sector developments;
- clarify the roles of Federal agencies concerning safeguard technology, particularly those of NSA and NBS;
- promote competition, innovation, and trade;
- separate, where practical, defense and intelligence agencies' missions from those of the private sector and civilian agencies; and,
- minimize or reduce the tensions between Federal policies and private sector activities.

The basic alternatives for policy center around the relative roles of NBS, NSA, and the private sector in providing leadership in the technological development and use of safeguards for unclassified electronic information. The options are:

> *Option 1.* Centralize Federal activities relating to safeguarding unclassified information in Government electronic systems under the National Security Agency.
>
> *Option 2.* Continue the current practice of de facto NSA leadership for communications and computer security, with support from the National Bureau of Standards.
>
> *Option 3.* Separate the responsibilities of NSA and NBS for safeguard development along the lines of defense and nondefense requirements.

The bill currently being considered by Congress (HR 145) is a variation of option 3 and is an attempt to resolve, by legislative means, policymaking for information security. One of its principal results is that it would clarify the roles of NBS and NSA, and tend to separate civilian and defense interests. Among its main shortcomings is the absence of a capability to support unclassified research in safeguard technology. This capability, perhaps more than any other single factor, would strengthen the ability of the private sector to satisfy its own needs for information security and reduce dependence on the Government.

In option 3, additional choices can be made.

> *A.* Provide Federal support to the private sector to specify, develop, and certify safeguards for business and civilian agencies. NBS would be the focal point for all safeguard standards for unclassified information; NSA would remain the focal point for classified information.
>
> *B.* Allow free market forces to develop safeguards for nondefense needs, with NBS acting as the focal point for Government needs for safeguards for unclassified information. NSA would satisfy the requirements of Department of Defense agencies and their contractors, and provide technical advice for other users.

Each of the three broad options has shortcomings. Essentially, the choice depends on whether policymakers prefer to tolerate greater tensions, a blurred division between defense-intelligence and civilian matters, and more constrained private sector technical capabilities, or to take larger risks that intelligence capabilities will be damaged by proliferation abroad of U.S. safeguard technology.

OTA's evaluation indicates that centralizing authority in NSA for developing safeguards for unclassified information in Government systems (option 1) or maintaining the current, blurred relationship between NBS and NSA (option 2) would be the least effective in minimizing tensions and in separating defense and intelligence missions from civilian matters. On the other hand, U.S. foreign signals intelligence gathering operations may be poorly served if NSA is not party to all safeguard development (option 3).

Independent of institutional arrangements in the United States, however, there are also risks to our intelligence that stem from sources outside the control of U.S. policy, such as the policies of foreign governments, actions taken by international business interests, and the effects of foreign innovation.

There are inherent tensions between U.S. intelligence interests and evolving nondefense needs for information security technology. In addition, there are enduring conflicts involved in balancing national security and broader national interests. Potential conflicts also exist between the tendency to restrict access to unclassified, but sensitive information, and concern for the free flow of information and constitutional rights. Perhaps the optimum result that legislation should be expected to achieve is to provide a clear policy basis against which to measure future imbalances.

In addition, any option that raises the cost of safeguards, impairs user operating efficiency, or results in incompatible standards for defense and non-defense users, will discourage the development and use of commercial products.

There are no options for Federal policy that clearly and simultaneously foster all national objectives without costs to others. The alternatives for implementing policy differ mainly in the source of national leadership for the development and nondefense use of safeguard technology, the level of Federal encouragement or control of private sector innovation, and in flexibility to adjust to changing needs of commerce and society.

For policies to meet the evolving needs of the Nation, they will have to be flexible and balance various national interests.

Three main observations result from OTA's analysis:

1. Excessive accommodation of either commercial or defense and intelligence concerns could prove damaging to overall U.S. interests.
2. Policies that are inflexible, based primarily on defense and intelligence interests or on Government control of technological advances in the private sector, are likely to create substantial tensions with the widening range of other national and international interests affected by them.
3. A process for weighing competing national interests is needed. Centering policymaking in the Department of Defense alone and, in particular, NSA would make that difficult.

Chapter 2

Introduction

CONTENTS

	Page
Society's Changing Needs for Information Security	13
Information Security and Government Policy	15
Importance of Information Security Technology and Policies	16
Business Interests in Information Security	19
Conclusions	19

Chapter 2

Introduction

> On a day nearly 4,000 years ago, in a town called Menet Khufu bordering the thin ribbon of the Nile, a master scribe sketched out the hieroglyphics that told the story of his lord's life and in so doing he opened the recorded history of cryptology.
>
> —David Kahn, *The Codebreakers: The Story of Secret Writing*

Information technology is revolutionizing society as profoundly as mechanical technology did in creating the industrial revolution. As a result, we are increasingly dependent for society's everyday functioning on electronic ways to gather, store, manipulate, retrieve, transmit, and use information. By all accounts, the importance of automated information systems and the communications systems that link them will continue to increase and transform the way we conduct our government, business, scientific, and even personal affairs.

This increasing dependence on information technology is creating a need to improve the confidentiality and integrity of electronic information, i.e., its security, so that computer and communications systems are less vulnerable to intentional and accidental error or misuse. This will allow us to use the new systems with confidence in a widening range of applications, such as electronic contract negotiations, with assurance that private, proprietary, or intellectual information entrusted to them will be properly protected.

Progress is being made in developing techniques for satisfying these needs. However, both the pace and direction of this progress will be affected by two factors:

- the traditional use of Federal information security policy, often as a means of implementing national security goals; and
- the need to accommodate the variety of national interests that are affected by Federal policy on information security.

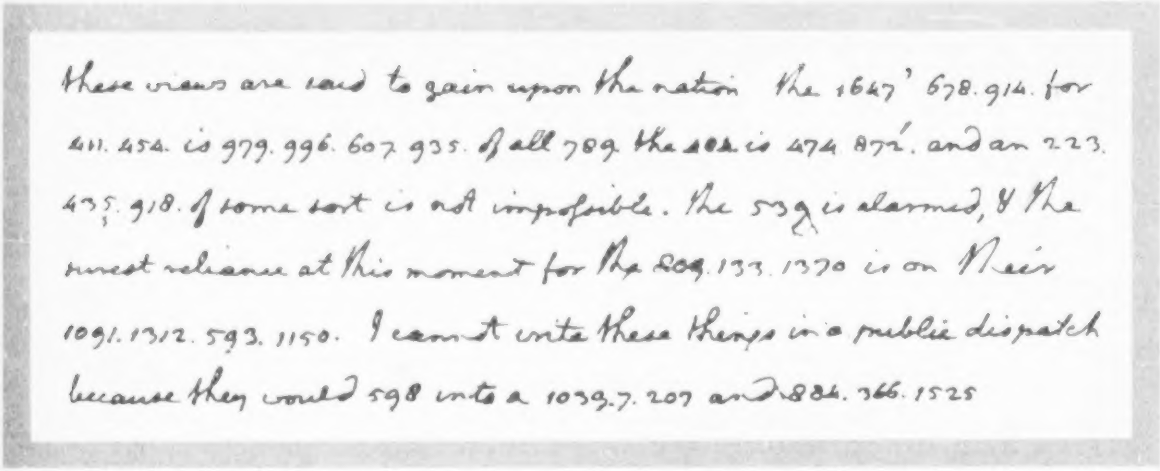
To put the topic in perspective, just as information security is a small, but vital part of the larger framework of information technology, Federal policy on information security is a reflection of broad national interests, rather than that of national security alone.

SOCIETY'S CHANGING NEEDS FOR INFORMATION SECURITY

The need for information security is not new. It dates back hundreds, even thousands, of years. Methods for conveying confidential messages were used in ancient Greece and much of the Western world by kings, generals, diplomats, and lovers. Today, the governments of most developed nations make extensive use of encoding techniques to keep their sensitive electronic communications secret.

Technology itself has long played a leading role in causing certain attributes of information security to become highlighted. The introduction of the telegraph brought concern about eavesdropping. Inexpensive sound and video recording capabilities raised concerns about unauthorized reproduction. And the proliferation of electronic storage quickly brought questions of how to prevent misuse of electronic data. Indeed, most of the attributes of information that are of concern today—confidentiality, accuracy, accountability—have long existed. Technological advances have not only modified their importance but have also introduced fundamentally new issues.

Today's technology provides new capabilities that raise both familiar and new concerns for security. High on the list of current concerns are the need for controls on capabilities for accessing, altering, and duplicating electronic data, and the ease of retrievability and



these views are said to gain upon the nation the 1647' 678. 914. for
411. 454. is 979. 996. 607. 935. of all 789. the 802. is 474. 872'. and an 223.
435. 918. of some sort is not impoſsible. the 539 is alarmed, & the
surest reliance at this moment for the 209. 133. 1370 is on their
1091. 1312. 593. 1150. I cannot write these things in a public dispatch
because they would 598 into a 1039. 7. 207 and 884. 366. 1525

Segment of original letter (top) and translation (bottom) from Thomas Jefferson to James Madison, August 2, 1787. Reproduced from *The Papers of James Madison*, vol. 10, 1787-1788, pp. 124-126. Library of Congress.

These views are said to gain upon the nation. The *kings passion* for *drink* is *divesting him* of all *respect*. The *queen* is *detested* and an *explosion* of some sort is not impossible. The *ministry* is alarmed, & the surest reliance at this moment for the *public peace* is on their *two hundred thousand men*. I cannot write these things in a public dispatch because they would *get* into a *newspaper* and *come back here*.

searchability of databases. Still other concerns include ensuring the accuracy of messages and verifying their origin, and providing means for auditing or reconstructing transactions. These concerns have arisen both in Government agencies and in businesses worldwide because traditional physical security measures are limited in their ability to prevent misuse of information in today's automated world.

In addition, as information technology increasingly substitutes for paper-based systems, it is important to retain familiar capabilities of the older technology. In fact, many of the developments in security are attempts to imbue in modern information systems parallels to the more familiar safeguards and procedures of paper-based and face-to-face forms of business transactions that we have become accustomed to using—as discussed later.

Some security techniques are adaptations of earlier ones, while others are genuine innovations. Modern equivalents of such traditional security tools as passwords, notary public "seals," codebooks, physical identification, separation of authority, and auditable bookkeeping procedures are all being used or considered today, separately or in combination, to contain misuse of electronic information. Prominent among the recent innovations are public-key cryptography, and the "zero knowledge" proof. The former may be used to establish private communications between previously unacquainted parties, as well as to provide the electronic equivalent of a personal signature. The latter can be used to demonstrate that a person knows a piece of information without revealing the information in the process. For example, it could be used to demonstrate knowledge of a solution to a "hard problem" without revealing anything about the specific solution method. Each of these innovations have broad implications for new applications of information technology.

Such encryption-based safeguards provide a basis for today's sophisticated information security technology and an expanding range of commercial applications. Banks are beginning to use these technologies to safeguard electronic fund transfers. Similarly, some companies are beginning to use them to protect the confidentiality of electronic mail and to replace paper-based business transactions with less expensive electronic equivalents. Expanding these capabilities to include proof of message receipt and acceptance, and protection of the anonymity of those taking part in transactions, is likely to require further innovation.

INFORMATION SECURITY AND GOVERNMENT POLICY

Federal policy for the security of electronic information was, until recently, an obscure topic having little public interest. In the first place, virtually all such policy was related to the secrecy of military, intelligence, and diplomatic information. Second, the authority and expertise for keeping information secure rested with defense and intelligence agencies that normally do not engage in open policymaking. Moreover, except for defense contractors, Federal policies had little effect on the public or on private businesses.

The Government's national security focus created an incentive to control the proliferation abroad of communications safeguard products and, in fact, to control the technology itself. The purpose was to deny foreign adversaries access to valuable U.S. technology and to protect the viability of U.S. foreign intelligence operations.

During the 1970s, the National Bureau of Standards (NBS) began to develop computer security standards for use by Government agencies based on its authorities stemming from the Brooks Act of 1965. In 1977, with technical assistance from the National Security Agency (NSA), NBS adopted the Data Encryption Standard (DES) as the national standard for cryptography. For the first time, a published cryptographic standard became available for civilian agencies, and it quickly was adopted by business users and the American National Standards Institute as the basis for many industry standards. NBS also began to validate commercial products implementing DES, thereby increasing users' confidence in the products' conformance with the Federal standard. As a consequence, DES is gradually becoming used for many applications.

Interest in information security is now worldwide and an active area of research and development in western European countries and Japan. DES has been considered as an international standard during recent years in forums composed of representatives from international businesses and governments (see ch. 5).

The proliferation of information technology has made more sensitive data accessible to more users, thereby creating another form of new vulnerability to misuse. In order to limit potential damage to U.S. interests, particularly from foreign intelligence agencies, the executive branch has sought to control access to unclassified information that it deemed sensitive. Although the definition of such information has been open to considerable debate that is still unresolved, it may include proprietary information filed with defense agencies and the Environmental Protection Agency, economic data collected by the Commerce and Treasury Departments, and personal data kept by the Department of Health and Human Services.

Policy directives issued by the executive branch in 1984 and 1986, and ensuing congressional hearings in early 1987, have significantly increased public concern over Federal information security policy. The expanding pattern of defense-intelligence interests as a central focus in the formulation of policy is seen as competing with other major national interests and has become the subject of public debate. The focus of the debate has been on the potential impact of these policies on some fundamental tenets of American government: the separation of and appropriate balance between defense and civilian authority, constitutional rights, open science, and Government controls on public access to information. The debate also raises the question of how to resolve conflicts involving the boundary between the authorities of the legislative and executive branches in making policy when national security is a consideration. On a more practical level, there are also serious misgivings about the applicability of the security approach taken by the Department of Defense (DoD) to the needs of the private sector.

At the same time that these Federal policies and their effects have been unfolding, trends are visible that may significantly influence commerce and other private sector interests.

IMPORTANCE OF INFORMATION SECURITY TECHNOLOGY AND POLICIES

Interest in information security technology now clearly extends beyond the Federal Government to the private sector as well. Its importance to business and society cannot be gauged adequately by the dollar amount of sales of products, but by the range of applications that the technology makes possible.

Safeguard technology is likely to become a mainstay for facilitating tomorrow's automated world of finance, commerce, and law, much as automated message authentication and verification are now becoming essential for the banking industry worldwide. These technologies are used to authorize transactions, authenticate users, verify the correctness of messages and documents, certify that legitimate transactions have occurred and identify the participants, and protect individual and corporate privacy.

Such applications are likely to be used to establish a legally valid electronic equivalent of the centuries-old, paper-based systems for authorizing access to information, identifying parties to agreements, authenticating letters and contracts, ensuring privacy, and certifying value. In this sense, they will replace such traditional safeguards as letters of introduction, signatures, and seals, and assume an importance difficult to foresee from the limited applications of today.

Both Government and industry are interested in improving the security of information they own or are entrusted with. Two major trends reflect these interests and are bringing attention to the direction of Federal policy. One concerns the Federal Government's need to keep an increasing amount of unclassified information confidential while, at the same time, gathering intelligence from other countries. The question of what information ought to be kept confidential, or have access to it controlled, is not well defined, but subject to judgments concerning potential damage to the Nation's security; examples of such information might include corporate proprietary data that could benefit foreign competitors or data useful to terrorists. The other trend is the evolving and growing need of the private sector to safeguard certain of its information and information resources from theft, destruction, or other misuse.

Federal policy has been formulated both by the executive and legislative branches, sometimes with similar purposes. Policy in information security has often been set by the President, based on national defense needs. This has invariably led to a major role for the DoD. Legislation, on the other hand, has also been used to establish policy for information security. The latter has often been based on other national interests, such as the privacy of telephone communications and of data in Government computer systems. Such laws typically have involved civilian agencies in their implementation.

Society's needs and the new demands stimulated by technology are causing these sepa-

Photo credit: Courtesy of NBC News Video Archive

Roof of Soviet embassy in Washington D.C. showing antennas

rate policy paths to converge. With this convergence, major stresses are becoming visible in the balancing of competing national interests and with the process by which policy is developed.

The focus of information security policy on the military, intelligence, and diplomatic interests of Government has particular significance for the issues of today for two interrelated reasons. First, responsibility for protecting the security of Government electronic information is consolidated within the defense and intelligence communities, where NSA has been given the lead responsibility. The second concerns the broadening scope of executive branch actions taken for reasons of national security. There is a tendency for this concern to include unclassified, but sensitive information.

NSA was created in 1952 as an agency of DoD by secret Executive Order. For decades its existence was not made public, and the only extensive public description of its operations were provided in the book, *The Puzzle Palace*, which the agency tried to prevent from being published.[1] NSA has been the subject of considerable controversy during the past decade due to its secret operations.[2]

NSA's functions are a consolidation of missions previously performed by each of the military departments. One of its two main missions is foreign signals intelligence, i.e., gathering information principally by intercepting and decoding electronic communications. It also protects U.S. military and diplomatic communications by enciphering them or making them less accessible to interception by the intelligence agencies of other countries. Such work is classified. NSA's work in developing encryption techniques, however, has made it the undisputed technical leader in the United States. More recently, the agency has widened its scope to include computer security.

Some of these Government efforts to reduce vulnerabilities from unauthorized access to communications systems are also creating tensions with other defense and intelligence interests. To the extent that methods to reduce unauthorized access to these systems enter the public domain, they can be used by other countries, thereby damaging NSA's ability to gather intelligence.

Since the 1970s, DoD has become increasingly concerned about the vulnerability of U.S. communications to foreign intelligence activities. As a result, NSA has launched several programs to better safeguard the Government's electronic communications. NSA has also encouraged domestic common carriers to provide tariffed "confidential" communications services for customers and has briefed dozens of U.S. companies on the vulnerability of communications systems to interception.

Second, where "national security" has generally been used to control classified military and certain diplomatic electronic information, executive branch directives of 1984 and 1986 extend this rationale to encompass unclassified information considered to be sensitive.

A current debate concerns the appropriate agency for Federal leadership for developing security standards for civilian computer systems—NSA or the Department of Commerce's NBS. However, the core issue is more basic. It goes to the question of whether or not a defense agency should control matters that are central to civilian interests, such as commerce and the free market, constitutional rights, and principles of open science. It also involves questions about executive branch authority under the Constitution to set policy based on national security. Yet a third dimension involves society's evolving needs for information security and the appropriate Federal role in accommodating those needs.

---

[1] James Bamford, *The Puzzle Palace* (New York, NY: Penguin Books, 1983).

[2] Ibid.

The event that triggered the current examination of Federal policy was the National Security Decision Directive-145 (NSDD-145), dated September 17, 1984. That executive branch directive established as Federal policy the safeguarding of unclassified, but sensitive information in communications and computer systems that could otherwise be accessed by foreign intelligence services and result in "serious damage to the U.S. and its national security interests."

NSDD-145 also created an interagency management structure to implement the policy. It gave leading roles to the National Security Council, DoD, and NSA. These roles include defining what information to protect, deciding on the appropriate technology for safeguarding unclassified information, developing technical standards, and assisting civilian agencies in determining the vulnerabilities of systems to misuse.

NSDD-145 raised numerous questions from critics in other Government agencies as well as from civilian sources, some of which relate to the broader issues mentioned above. They include concern for:

- intermingling defense and civilian matters;
- public access to Government information;
- the legislated responsibility of NBS to develop computer standards for the Federal Government under the Brooks Act of 1965, as amended;
- private sector development and use of safeguard technology; and
- expanding the responsibilities of NSA in civilian matters, particularly in light of the conflict of interest between its intelligence mission and commercial needs, and its lack of direct public accountability.

The level of public concern was elevated further with the release by the National Security Council in October 1986 of a policy statement defining what information is sensitive and therefore possibly in need of safeguarding.[3] The release coincided with well-publicized Government activities aimed at identifying and possibly restricting access by selected foreign governments to unclassified, but sensitive data in Government and commercial automated information systems. As a result, the issue of Government restrictions on public access to unclassified information, whether or not in Government systems, has become a public concern. The statement, though rescinded in early 1987, caused public alarm that illustrated the extent of sensitivities among diverse organizations concerning controls on unclassified information.

Perhaps the major effect of these executive branch policies to date has been to encourage an examination by Congress of the effects of such defense-oriented policies on civilian matters. Legislation has been proposed to reestablish civilian control over the security of unclassified information systems. In the short term, many of the currently prominent issues related to information security policy are likely to be addressed by congressional debate over the proposed legislation, including the respective roles of NBS and NSA in setting standards and the measures to be taken, if any, to control access to unclassified information.

For the longer term, however, the vulnerabilities to misuse of information systems will depend on the development and widespread use of technical, administrative, and related safeguards. The availability of high-quality information safeguards worldwide, especially cryptographic-based systems, on the other hand, will make intelligence gathering more difficult for the United States.

---

[3] National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, National Security Council, Oct. 29, 1986.

BUSINESS INTERESTS IN INFORMATION SECURITY

The question of the extent to which information systems should be protected depends on the various perceptions of threats to those systems. Simply put, U.S. defense and intelligence agencies are concerned about unauthorized access to commercial communications and computer systems by the intelligence organizations of foreign countries, particularly the Soviet Union. However, U.S. businesses or civilian agencies generally do not consider their main risk to be from such sophisticated adversaries.

The range of threats to business information systems is not as broad as that faced by defense and intelligence agencies. Business' concerns for misuses are mainly by insiders, competitors, and, to a limited extent, hackers.

Companies that safeguard their communications seem either to have business interests at risk (e.g., banking and oil exploration firms concerned about unauthorized interception) or are required by the Government to use prescribed safeguards (e.g., Federal Reserve banks and defense contractors). A number of businesses are finding additional reasons to provide some safeguards for information in computers and communications systems. These reasons include prudent management of resources and methods of improving efficiency, as well as preventing the loss of proprietary information or theft of funds. Private businesses, in addition, often are more concerned with information integrity rather than confidentiality.

For their part, businesses need safeguards that do not unduly slow down or otherwise impair normal business operations; that is, in order to be useful, security measures must be practical and efficient. U.S. firms engaged in international commerce and banking, to be able to use these systems, also must be able to export them to their subsidiaries in other countries.

Concern for cost is an area in which contrasts between defense and intelligence agencies and business interests are even more apparent. Private businesses must remain profitable and competitive, and, therefore, they resist safeguards unless they are cost-effective. Defense and intelligence agencies, because of their missions, are more tolerant of higher costs or of operational impediments that might result from adopting security measures. One of their most important goals is to prevent valuable information from falling into the wrong hands, even if significant trade-offs are involved.

Nevertheless, there are many similarities between the various defense and nondefense, as well as between Government and private sector, requirements for information security, although their requirements vary widely. Both need to control access to databases, restrict unauthorized activities, provide audit capabilities, safeguard sensitive data and transactions, and, generally, maintain the integrity of data and continuity of service. Thus, Federal policies that affect the longstanding NBS and NSA roles in developing technology to safeguard information systems will also affect private sector security programs.

CONCLUSIONS

The need for information security has existed for a long time. The particular attributes of security perceived to be important tend to change emphasis with time and technology, often in ways that are difficult to predict with confidence. Society's ability to satisfy its changing needs for improved security depends on its ability to adapt existing technologies and techniques as well as to innovate (see ch. 4). Government policy can be an important determinant of how, when, and by whom these needs are satisfied.

These conclusions imply that policies predicated solely on solving current security problems are not likely to endure because needs for information security are not static. Further, those based on controlling or restricting private sector actions are likely to damage other societal needs. In other words, flexibility and balance are important objectives of any policy intended to accommodate a wide range of users' needs on a continuing basis. Moreover, it seems apparent that U.S. policies that cannot effectively be enforced internationally risk being overcome by events in other countries.

Further, information security policy has a significance that is colored by different interests. One view sees its significance as relating mainly to the potential for foreign government intelligence via U.S. communications and computer databases and other threats to national security. From a different viewpoint, however, the significance of information security involves even more diverse interests. These include basic democratic principles and civil liberties, as well as commercial business interests.

In addition to these interests, each of which has its advocates, there is at least one other that has no clear advocate—the evolving needs of society for information security. Society's needs for information security has a long history that is continually evolving. Federal policy also has an influence on advances in the technology underlying information security applications, especially when the technology itself is controlled for national security purposes.

Regardless of the viewpoint taken, information technology poses a challenge to Government, industry, and society. Modern information systems and the data within them are vulnerable—they can easily be misused. The challenge is to find ways to reduce the risks to acceptable levels while preserving traditional democratic values and remaining flexible to accommodate diverse and changing needs.

The remainder of this report examines some of the technological foundations for information security and the main policy issues that are now evolving. In order to focus attention on the issues facing Congress, many topics have been treated in a limited way. The report is not about potential disruptions to or recovery from disasters, for example, nor is it about physical security or safeguarding classified information or constitutional rights. Its purpose, instead, is to describe the conflicting national interests that are shaping U.S. information security policies, the special role of cryptography and NSA's intelligence mission, and the potential courses of action.

Chapter 3

The Vulnerabilities of Electronic Information Systems

CONTENTS

Page
Findings 23
Introduction 23
Vulnerabilities of Communications Systems 24
  Background 24
  Spectrum of Adversaries' Resource Requirements 27
  Networks 28
  Transmission Systems 29
  Other System Components 37
  Commercial Availability of Interception Equipment 38
Vulnerabilities of Computer Systems 39
  Background 39
  Large-Scale Computers 39
  Microcomputers 41
  Software 42
  The Extent of Computer Misuse 44
Typical Vulnerabilities of Information Systems 44

Boxes

Box *Page*
A. Examples of Historical Concerns for Misuses of Telecommunications Systems 25

Figures

Figure No. *Page*
1. Spectrum of Adversaries' Resource Requirements v. Technologies 28
2. The Communications Network 30
3. Example of Antenna Directivity Pattern 32
4. Examples of Commercial Equipment for Interception of Microwave Radio Signals 33
5. Typical Fiber Optic System 35
6. Mainframe Computers in Federal Agencies 40
7. Computer Terminals in Federal Agencies 41
8. Trends in Component Density, Silicon Production, and Gallium Arsenide Announcements, 1960 to 1990 42
9. Microcomputers in Federal Agencies 43
10. Typical Vulnerabilities of Computer Systems 45
11. Technical Safeguards for Computer Systems 47

Tables

Table No. *Page*
1. Bell System Circuit Miles of Carrier Systems Using Different Transmission Media 29
2. Telephone Company Fiber Applications 34
3. Sales of Large-Scale Host Computers in the United States 40
4. Sales of Personal Computers in the United States 42

Chapter 3

The Vulnerabilities of Electronic Information Systems

FINDINGS

- Today's public communication network is, for the most part, at least as easy to exploit as at any time in the history of telecommunications. The design of the public switched network is such that some parts of it are vulnerable to relatively easy exploitation (wiretaps on copper cable, over-the-air interception), while others (e.g., fiber optic cable) present greater inherent barriers to exploitation.
- There are, and will likely remain, opportunities for casual, generally untargeted eavesdropping of communications. However, targeted and consistently successful unauthorized access requires greater resources. For systems with sophisticated safeguards, the resource requirements may frustrate even the efforts of national intelligence agencies. However, adversaries with sufficient resources can eventually defeat all barriers except, perhaps, those based on high-quality encryption.
- Users of communications systems face a spectrum of vulnerabilities ranging from those that can be exploited by unsophisticated, low-budget adversaries to those that can be exploited only by adversaries with exceptionally large resources.
- Technological advances may increase the capabilities of adversaries to misuse computer and communications systems, but these same advances can also be used to enhance security.
- Increases in computing power and decentralization of functions have increased exposure to some threats. Two types are important: abuse by intruders who are not authorized to use or access the system, and misuse by authorized users. For many organizations, the latter problem is of most concern.

INTRODUCTION

Unauthorized disclosure, alteration, or destruction of information in computer and communications systems can result from technical failure, human error, or penetration. While each of these is important to users, this chapter focuses on malicious or deliberate unauthorized access and alteration, principally because it is in these areas that the impact of Federal policies is greatest.

Widely different levels of time, money, and technical sophistication are needed to gain unauthorized access to different parts of communications and computer networks. Some forms of covert access—placing wiretaps, intercepting mobile telephone calls, hacking into poorly safeguarded computers—require few resources. Others, such as targeted and consistently successful unauthorized access, require greater resources because of the inherent barriers posed by the complex designs of these systems. For systems with sophisticated safeguards, the resource requirements may frustrate even the efforts of national intelligence agencies.

Today's communications networks make use of diverse technology. This diversity is accompanied by an uneven ease of unauthorized access to different parts of the system. Although security has not been a consideration in network design, today's systems provide some inherent barriers to easy exploitation. However, adversaries with sufficient resources can eventually defeat all barriers, except perhaps high-quality encryption.[1] Information in computers also has been vulnerable to malicious disclosure or alteration by various methods of penetration, including misuse by both authorized and unauthorized users. However, significant advances are being made in the technology available for safeguarding computer and communications systems, as discussed in chapter 4.

Many users of communications and computer systems remain unaware or unconvinced of significant threats due to such vulnerabilities. Most users are not now adding safeguards, despite the growing volume and value of information being stored in or transmitted across these systems.

Computer and communications systems are becoming increasingly closely intertwined. Consequently, information security is affected by the operation of all segments of these systems. Communication networks pose one set of vulnerabilities to misuse that centers around unauthorized disclosure of information and to modification of data. When computers are linked by communications networks and are remotely accessible, the potential for misuse increases.

This chapter focuses primarily on the vulnerabilities to misuse of communications systems and methods to safeguard against them. It is intended to raise awareness and understanding of some of the technical vulnerabilities of these systems without providing a cookbook for prospective exploiters.[2] Because communications and computer designs and applications vary widely, their vulnerabilities are described in general ways in the sections that follow.

---

[1] For the purposes of this report, high-quality encryption techniques, for which there are no known and significant weaknesses or deciphering shortcuts, are considered to be fully secure, in spite of the fact that trial-and-error attacks will yield the unenciphered text (plaintext) with a sufficient number of trials.

[2] Although not the subject of this report, it should be noted that simpler and often less expensive ways than electronic eavesdropping can be used to gain access to sensitive information; i.e., by bribing employees or by using spies. Thus, users considering adopting electronic security measures must weigh all sources of potential losses, including those from human and other errors, as well as from dishonest employees.

VULNERABILITIES OF COMMUNICATIONS SYSTEMS

Background

The developed world has become increasingly dependent on communications systems to operate businesses and governments at all levels. This can be seen in the revenue growth of communications services. The operating revenues from the domestic services of common carriers, for example, grew from $8.4 billion in 1960 to $166.5 billion in 1985. Similarly, revenues for domestic satellite services rose from near zero in 1975 to $17 billion in 1985. And Intelsat's revenues from international services went from near zero to $475 million in the past two decades.

The growth in revenues reflects the fact that communications networks have become vital for many purposes, ranging from making interbank and government fund transfers to running national electric power grids and the world's airlines. There is every indication that this dependence will increase with continued advances and new applications. Both the volume of information communicated and its importance will continue to grow.

There have been occasional concerns about the vulnerability of telecommunications systems to misuse. Illustrations of some historical concerns and examples of misuse during the past century are shown in box A. Although today's systems are likewise vulnerable to misuse, commercial demand for improved security (e.g., message confidentiality and integrity) has been slow to materialize. Nevertheless, message authentication and digital signature capabilities are becoming important for a number of industries (see ch. 5).

Little has been done to improve the security of public communications systems themselves. Generally, commercial systems have been designed for efficiency and reliability rather than security. Also, their inherent barriers to misuse adequately serve most users' needs for confidentiality. Where additional safeguards are deemed necessary, "add-on" measures are taken either by the user directly (adding encryption or message authentication capabilities), through the special service options offered by some communications carriers (see chs. 4 and 5), or by a combination of administrative procedures and the use of a protected private communications network.

The regulatory climate has also influenced the confidentiality of systems. The communications industry now faces an increasingly deregulated environment created, in part, by the divestiture of the American Telephone &

Box A.—Examples of Historical Concerns for Misuses of Telecommunications Systems

- In 1845, only one year after Samuel F. B. Morse's famous telegraph message "What hath God wrought," a commercial encryption, or encipherment, code was published as a means of ensuring secrecy.[1]
- The first voice scrambler patent application was dated within 5 years of the first demonstration of the telephone in 1881.
- During the Civil War, "the first concerted efforts at codebreaking and communications system penetration, or telegraph line tapping were undertaken."[2]
- Soon after radio communications came into use in 1895, they were used for intercepting others' messages, particularly before and during World War I.[3] In the 1920s, the British surreptitiously eavesdropped on international cable traffic.[4]
- The diversion of an undertaker's business by an eavesdropping switchboard operator resulted in a patent grant for design of the first automatic switch in 1891, eventually eliminating the need for switchboard operators.[5]
- During the 1920s, pervasive Government and criminal use of telephone wiretaps triggered congressional hearings and antiwiretap legislation.
- Interception of telecommunications signals played a key role in the course of World War II. It continues to be a source of foreign intelligence gathering by major governments.[6]
- In recent years, there has been concern about the ease of misuse of a variety of telecommunications signals, ranging from the pirating and even malicious jamming of subscription television signals transmitted over satellite communications systems to the ease of interception of cellular radio and mobile radiotelephone signals.[7]

---

[1] David Kahn, *The Codebreakers: The Story of Secret Writing* (New York, NY: MacMillan, 1967), p. 189.

[2] Supplementary Reports on Intelligence Activities, Book VI, Final Report of the Select Committee to Study Government Operations with respect to Intelligence Activities, U. S. Senate, Apr. 23, 1976, p. 51.

[3] Kahn, op. cit., pp. 298-299.

[4] James Bamford, *The Puzzle Palace* (New York, NY: Penguin Books, 1983), pp. 29-30.

[5] John Brooks, *Telephone: The First Hundred Years* (New York, NY: Harper & Row, 1976).

[6] Kahn, op. cit.; Bamford, op. cit.; Peter Wright, *Spy Catcher* (New York, NY: Viking Penguin, Inc., 1987); also see Glen Zorpette (ed.), "Breaking the Enemy's Code," *IEEE Spectrum*, September 1977, pp. 47-51.

[7] "HBO Piracy Incident Stuns Other Satellite Users," *New York Times*, Apr. 29, 1986, p. C17; "Look! Up in the Sky!" *Washington Post*, Apr. 29, 1986, p. C1; "Mystery Broadcast Overpowers HBO," *The INSTITUTE*, vol. 10, No. 10; October 1986, p. 1; "Uplinks and High Jinks: Satellites Are the Hackers Next Frontier," *Newsweek*, Sept. 29, 1986, pp. 56-57.

Telegraph Co. (AT&T) in January 1984. As a result, cost competitiveness has become an important consideration for communications carriers. It discourages them from providing cost-incurring safeguards for which there is no significant demand. A 1980 survey found that, with few exceptions, the Nation's 10 largest common-carrier systems were not designed for securing messages against interception. On the other hand, at least one carrier did offer an add-on encryption service.[3] A 1986 OTA review of six carrier systems indicates that a combination of protective services are becoming available, including encrypting radio signals or routing selected calls over cable transmission facilities.[4]

Technology plays an important but uneven role in the security of communications systems. The rapid proliferation of ground-based or terrestrial microwave radio since the 1940s and satellite communications since the 1960s have made interception easier by making signals available over wide geographic areas. Other technical designs have also made interception easier. Private lines (dedicated channels) and cordless telephones, for example, can be intercepted because of the former's fixed position in the electromagnetic spectrum and the latter's complete dependence on radio waves.[5] Telephone lines can also be tapped relatively easily from wire closets on a user's premises.[6]

Local area networks (LANs), which already have wide use in the United States and abroad for linking computer-based systems, represent another area of information technology in which security has received little attention. The same technologies that make possible continued improvements in computer and communications systems can also provide the means for sorting rapidly through a multitude of signals in search of specific telephone numbers, spoken words, or even voices.[7]

At the same time, technology and engineering can complicate the interceptor's work. Fiber optics, which is rapidly being installed in the United States to carry telephone and other communications,[8] requires far more sophistication for successful interception because of the physical medium that carries the message. However, most customers will continue to have copper wires linking their offices and residences with the local telephone company's office for the long term.

AT&T's modern electronic switching network, on the other hand, encrypts signaling information (the numbers of the called and calling parties) prior to transmission, thus denying potential interceptors the opportunity to target specific users' messages. Many other engineering design features, such as signal compression, spread-spectrum techniques, channel demand assignment techniques, and packet switching also complicate any interceptor's work. They do so typically as a byproduct of other objectives. And, within the next few years, as end-to-end digital networks become more commonplace, encryption services are likely to become available if demand is adequate. Of course, adversaries with significant resources, such as a national intelligence organization, can be expected to readily surmount most of these obstacles.[9]

---

[3] U.S. Department of Commerce, National Telecommunications and Information Administration, "Identification of Events Impacting Future Carrier System Protections Against Vulnerabilities to Passive Interception," 1980.

[4] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems," OTA contract report, 1986.

[5] For a description of the vulnerabilities of commercial telecommunications systems to unauthorized use, see the MITRE Corp., *Study of Vulnerability of Electronic Communication Systems to Electronic Interception*, vols. 1 and 2, January 1977; and the MITRE Corp., *Selected Examples of Possible Approaches to Electronic Communication Interception Operations*, January 1977. Also, Ross Engineering Associates, "Telephone Taps," OTA contract report, November 1986.

[6] Technical course material from a seminar on communication and information security, conducted regularly by Ross Engineering Associates, Adamstown, MD, and other firms. For additional information on wiretaps, surveillance, and related topics, see: "Electronic Eavesdropping Techniques and Equipment," Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, republished by Ross Engineering Associates. Also, Robert L. Barnard, *Intrusion Detection Systems: Principles of Operation and Application* (Stoneham, MA: Butterworth Publishers, 1981).

[7] Whitfield Diffie, "Communications Security and National Security: Business, Technology, and Politics," *Proceedings of the National Communications Forum*, Chicago, IL, 1986, vol. 40, Book 2, pp. 733-751.

[8] Bellcore, "Evolving Technologies: Impact on Information Security," OTA contract report, Apr. 18, 1986. Also, see U.S. Congress, Office of Technology Assessment, *Information Technology R&D: Critical Trends and Issues, Case Study 2: Fiber Optic Communications* (Springfield, VA: NTIS #PB 85-245660/AS, February 1985), pp. 67-75.

A number of recent developments may also be making it more difficult to intercept, alter, or misuse signals. These include the advent of commercial encryption services and products, the emergence of new technical standards for safeguarding communicated and stored messages, recent Federal Government policies that influence the safeguarding of sensitive information, and congressional legislation concerning unauthorized access to information in some systems (see chs. 4 through 6).

Still another barrier exists to the misuse of data obtained from passively monitoring or intercepting automated information systems—the problem of obtaining unambiguously the information of direct interest. This is readily illustrated with an example of data in the form of passively intercepted communications signals. Even if an adversary is reasonably assured that the intercepted signals contain useful data among them, the adversary must select from what may be a wealth of transmitted data in the hope of finding the target information in a timely, complete, and understandable context. Although these barriers are not likely to prove overwhelming to a determined, sophisticated adversary, they do not exist for an adversary who has the cooperation of a knowledgeable inside employee with the ability to select exactly the information of direct interest and with a full understanding of its context and limitations.

Spectrum of Adversaries' Resource Requirements

Telecommunication systems are vulnerable to unauthorized access in many ways, but the ease of such access varies widely depending on the resources available to potential adversaries. Targeted, unauthorized access to a specific user's communications over the public switched network, with a few exceptions, considerably increases the need for technical expertise, sophisticated equipment, and money. The complexity of these systems can prevent unsophisticated adversaries who lack the necessary resources from gaining access to information, but would not stop those who have adequate resources from readily surmounting the barriers.

Figure 1 illustrates the spectrum of vulnerabilities and adversaries' resource requirements. On one extreme are readily exploitable services (cordless telephones) and facilities (copper wire in local loops and wire closets) that require very limited resources for successful, targeted exploitation. Some cordless telephone conversations can be monitored using ordinary FM radios. Cellular radiotelephone conversations can be monitored using tunable ultra high frequency (UHF) television receivers. Further, wiretapping equipment can be purchased for as little as $12. At the other end of the spectrum are applications and facilities, such as fiber optic communications and technologies, particularly those using high-quality encryption and other safeguards (see ch. 4), that make unauthorized access much more difficult.

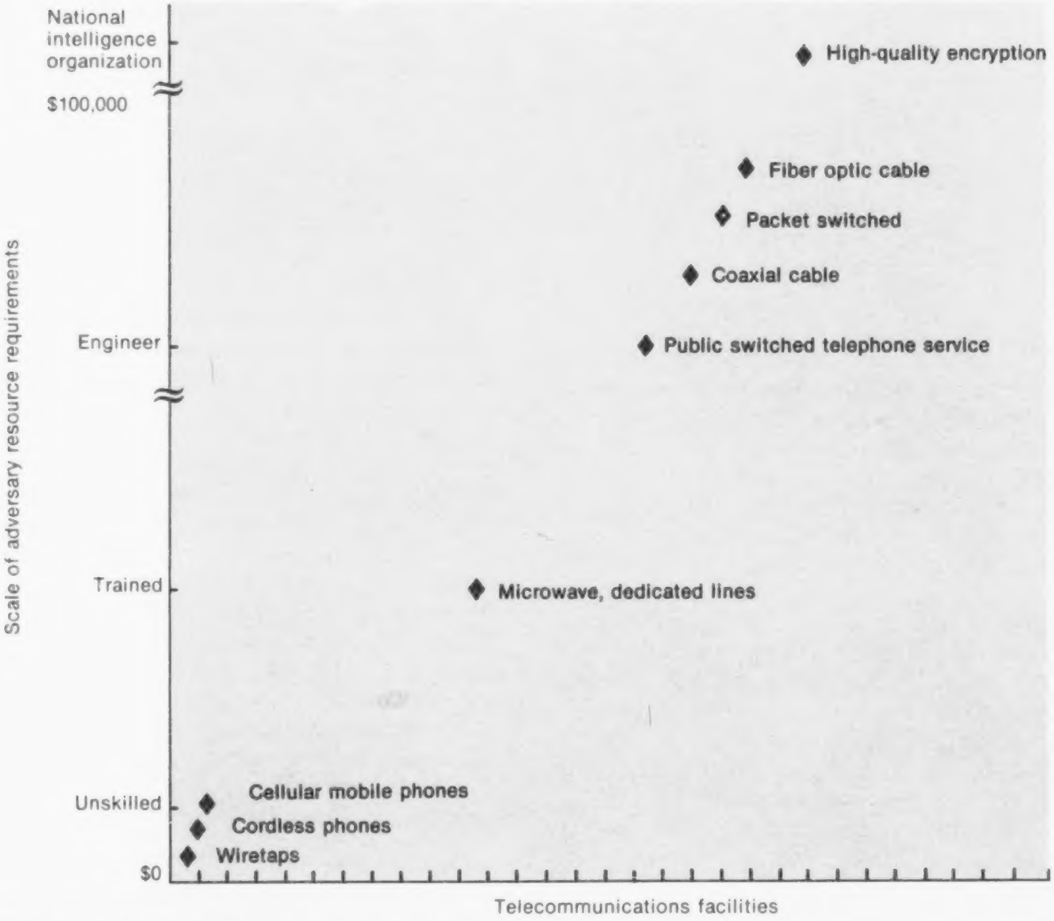
On the other hand, technology may simplify targeted interception through such means as computer-based data matching, word recognition, and voice identification. For most users, concern about unauthorized access is more likely to focus not on potential high- or low-resource adversaries, such as wiretappers or Government intelligence agencies, but on those in between.

The situation is far from a static one. The spectrum of vulnerabilities shifts as technological advances change the nature of communications systems and the resources available to potential adversaries. Technological advances, other than those associated with information security, tend to increase the capabilities of adversaries, especially those of high- and middle-level resources. Perhaps the most

---

[9] David Kahn, *The Codebreakers: The Story of Secret Writing* (New York, NY: MacMillan, 1967); James Bamford, *The Puzzle Palace* (New York, NY: Penguin Books, 1983); "Soviets Take the High Ground, New Embassy on Mount Alto is a Prime Watching and Listening Post," *Washington Post*, June 16, 1985, p. B1; and *The Soviet-Cuban Connection in Central America and the Caribbean*, released by the Departments of State and Defense, March 1985, Washington, DC, pp. 3-5.

Figure 1.—Spectrum of Adversaries' Resource Requirements v. Technologies



SOURCE: Office of Tecnnology Assessment, 1987.

visible illustration of this is that of increasingly powerful personal computers, which make unauthorized access to communications and data easier.

But the question remains: Should a business that communicates valuable, sensitive, personal, or proprietary information be concerned about unauthorized access to messages transmitted over the public switched network? If history serves as a guide, we can expect few immediate changes in the confidentiality of private communications over public networks except where user demand is adequate to justify investment in safeguards. However, some corporate and Government users who face considerable risk in the event of such accesses (e.g., for communications deemed sensitive for national security purposes or for electronic fund transfers) are taking steps to improve the confidentiality and integrity of their communications (see ch. 5).

Networks

Early communications networks began as relatively simple point-to-point transmission systems. At first, telegraph and later voice-modulated electronic signals, were transmitted exclusively over copper wires, and switching was accomplished manually. Such networks were vulnerable to eavesdropping by wiretapping. Today's networks, by contrast, consist of cables (copper wire, coaxial, and fiber optic), radio links (terrestrial and satellite), and other equipment providing a complex mix of services (voice, data, graphics, text, and video) through a variety of specialized interconnected networks. Figure 2 illustrates the complexity of modern networks. In spite of the added complexity, however, vulnerabilities remain.

Communication networks have also vastly expanded the ability of users, whether from an office building or home personal computer, to gain access to computers nationwide and even worldwide. The current movement toward a worldwide digital network is aimed precisely at increasing the accessibility of network capabilities, enhancing the variety of services available, and lowering the costs of services.

Transmission Systems

Communications systems use two types of media to transmit signals: over-the-air systems, such as radio transmissions; and conductors, such as copper wire and coaxial or fiber optic cables. In general, over-the-air systems (e.g., cordless telephones) can be intercepted and systems that use conductors can be tapped. Some conductor-based transmission systems (e.g., fiber optic cable) require sophisticated resources to tap, while others require minimal resources (taps of copper wires from wire closets). Whatever the form of transmission, it is not necessarily easy to render intercepted or monitored signals intelligible.

Microwave Radio Systems

Microwave radio systems, totaling 740 million circuit miles, carry most of the long-distance communications messages transmitted within the United States (table 1).[9] Systems operating at frequencies mostly between 2 and 11 GHz (gigahertz or billion cycles per second), for example, provide high-capacity circuits that carry about two-thirds of all telephone toll calls today. They often use highly directional antennas to transmit signals between stations, typically spaced from 10 to 35 miles apart.

Microwave systems are designed for a wide range of capacities, from as few as 24 voice grade circuits to as many as 2,400 circuits per radio channel. In addition, there are multiple radio channels in each of the many frequency bands that these systems operate in. For example, in the 6 GHz common carrier band, there are eight radiofrequency channels, each capable of carrying 2,400 voice grade circuits.

Interception of point-to-point microwave transmissions is relatively easy if the interceptor has technical information about the transmitter. Most such information is made available to the public by the Federal Communications Commission (FCC). Interception of signals, however, is only part of an eavesdropper's job. The signals must be demodulated and demultiplexed, which can be done using the same type of equipment as used by common carriers. But then an eavesdropper must also be able to sort through individual messages and select those of interest.

Table 1.—Bell System Circuit Miles of Carrier Systems Using Different Transmission Media

	Circuit miles at year end (in millions)	
Media	1975	1982[a]
Analog:		
Paired wire	42	140
Coaxial cable	142	221
Radio	399	737
Digital:		
Paired wire	58	138
Coaxial cable	—	2
Radio	—	6 (62% installed in 1982)
Fiber optic	—	4 (98% installed in 1982)
Subscriber	—	8 (54% installed in 1982)

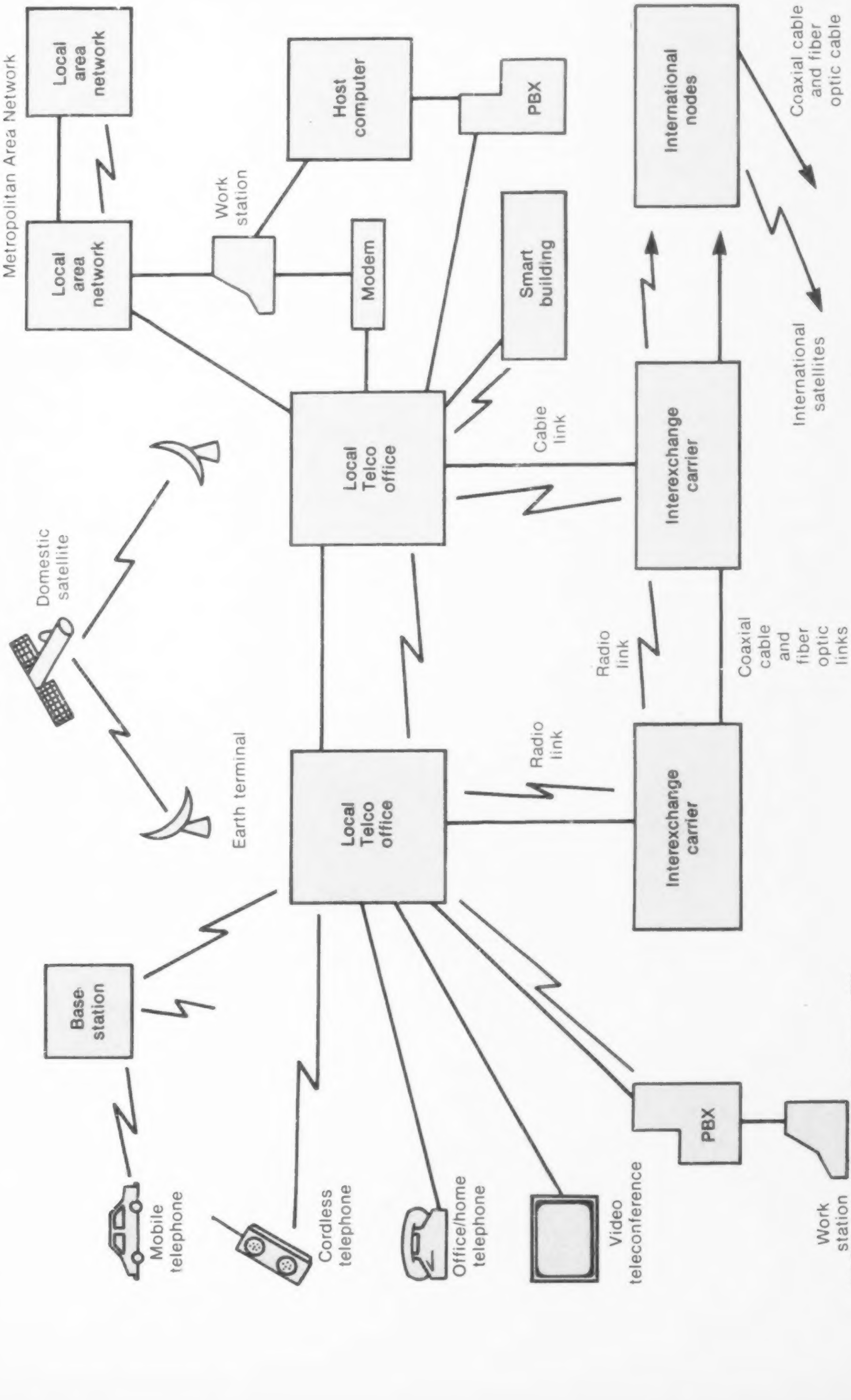
[a] This list shows major categories of transmission media. Although analog systems were still predominant, the growth of digital systems was almost three times faster from 1975 to 1982. Almost no new analog systems were added during this period. Comparable information is not available after 1982, but a significant commitment is being made to glass fiber systems, especially by AT&T, MCI, and GTE.

SOURCE: Bellcore.

---

[10] Bellcore, *Evolving Technologies: Impact on Information Security*, Apr. 18, 1986.

Figure 2.—The Communications Network



SOURCE: Office of Technology Assessment, 1987.

Point-to-point systems are vulnerable to interception wherever there is sufficient radiated signal strength. The geographic area in which adequate signals can be received is generally very large. It can cover dozens of square miles in the paths of the antenna's radiation and in the vicinity of either the transmitter or receiver (figure 3). Custom-built receivers may be designed with greater sensitivity than those used by the common carriers in order to broaden the area of reception.

Modern digital systems complicate interception by unsophisticated adversaries, but they simplify the work of those that are more sophisticated. Signals are transmitted as virtually indistinguishable series of ones and zeroes, typically mixed together (multiplexed) with many other signals and encoded prior to transmission to reduce the total number of bits transmitted and thereby reduce bandwidth requirements. Many systems also route different segments of the same transmitted signal over different paths. For adversaries with few resources, these conditions alone would represent significant obstacles, particularly for targeted interception.[11] Other obstacles include the need to record a large volume of data and process it to extract the message content.

For adversaries with considerable resources, such as very powerful computer processing capabilities and the equivalent of the switching and transmission facilities used by common carriers, targeted interception would not represent a severe challenge. Indeed, these adversaries can sort messages to select those of interest and undo the various types of signal processing to recover the message content. To consistently intercept preselected targets in switched systems, potential adversaries must be able to carry out functions equivalent to those performed by the carriers' equipment. In addition, they need the ability to select those messages of interest and to operate covertly. This level of sophistication and investment is assumed to be beyond the means of any adversaries except those with considerable resources and motivation, principally because of the cost of such an operation.

At the other extreme, there is inexpensive commercial equipment that can be used to intercept radio signals.[12] Figure 4 illustrates the types of equipment needed and current prices, based on catalog advertisements. The equipment includes an antenna that can be pointed, low-noise amplifier, receiver, and equipment to extract audio (and video) signals (i.e., demultiplex and demodulate them). Depending on the particular equipment selected, the total price would range from $1,000 to $50,000. People skilled in the design of communications equipment could undoubtedly build their own units for less, however.

Specialized Microwave Systems

The Multipoint Distribution Service (MDS), authorized by the FCC in the early 1970s, uses broadcast microwaves to distribute video and other one-way communications locally. MDS transmitters use omnidirectional antennas to broadcast signals that are received by small parabolic (directional) antennas. MDS systems are typically used as a radio version of cable television and, infrequently, to provide one-way business or educational communications.

A Digital Termination System (DTS) is another specialized microwave radio service that is similar to MDS in terms of its broadcast of microwave signals. However, unlike MDS, DTS is designed for full two-way communications between stations. The mechanics of intercepting DTS transmissions are similar to those involved with MDS or point-to-point microwave systems. Interception might be considered easier with DTS because of the clearer identification of the user's dedicated communications channel.

Dedicated Lines

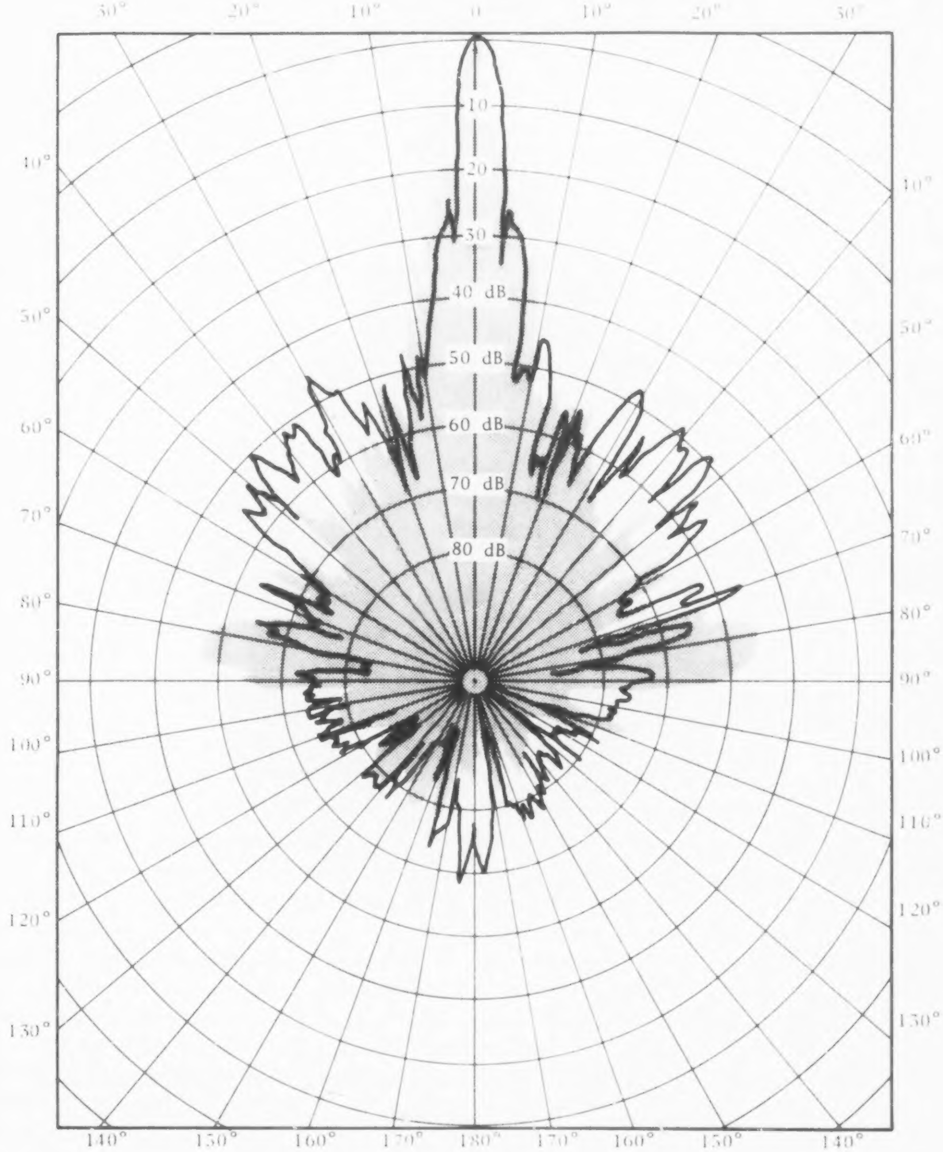
Users who need to communicate extensively between two points often use dedicated or pri-

---

[11] The MITRE Corp., *Study of Vulnerability of Electronic Communication Systems to Electronic Interception*, vol. 1, January 1977, p. 96.

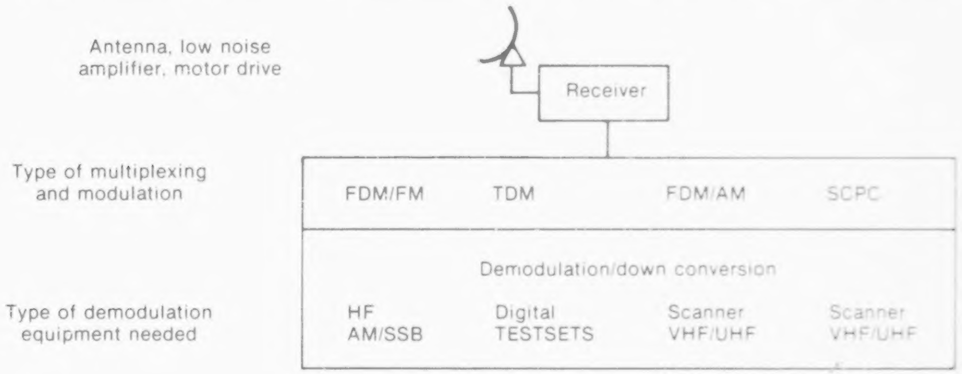
[12] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems," OTA contractor report, 1986.

Figure 3.—Example of Antenna Directivity Pattern



SOURCE: MITRE Corp., *Study of Vulnerability of Electronic Communication Systems to Electronic Interception*, vol. 1, January 1977

Figure 4.—Examples of Commercial Equipment for Interception of Microwave Radio Signals


Antenna, low noise amplifier, motor drive
Receiver
Type of multiplexing and modulation
FDM/FM
TDM
FDM/AM
SCPC
Demodulation/down conversion
Type of demodulation equipment needed
HF AM/SSB
Digital TESTSETS
Scanner VHF/UHF
Scanner VHF/UHF

	Commercial equipment	Approximate price
Examples of Receiving equipment, Low noise amp., Motor drive	RAYDX 10.5' antenna, LUX or 990C receiver	$2,200 Good quality reception
	ALCOA 6.0' antenna, Uniden 2000 receiver	$695 Minimum quality reception
Examples of Demodulation Equipment	HF-AM/SSB ICOM R7000	$969
	HF-AM/SSB BEARCAT DX1000	$285
	VHF-UHF Scanner Regency MX5000	$330

Total system cost: Between $1,000 and $3,200

SOURCE: Information Security Inc., using catalog prices from SATCOM, and SCANNER WORLD USA magazines, 1986.

vate line services. These are fixed circuit paths through some combination of terrestrial or satellite microwave radio or wire transmission facilities. Dedicated lines are commonly used to link corporations' main switching centers with one another, to link interactive computer systems, and to link computer systems with remote terminals. Whereas ordinary dial-up calls might be routed along any of a number of paths depending on traffic loading conditions, dedicated circuits remain in place on the same transmission path. This simplifies the interceptor's burden considerably, since the location of the user's dedicated line need be found just once. As an example of a part of a dedicated circuit, the local loop connecting the subscriber's premise with the local telephone company's nearest office also provides a fixed path that is relatively easy to identify.

Fiber Optic Communications

Fiber optic cable is being installed rapidly by communications carriers in the United States, primarily for heavy traffic, long-distance routes, but also for many local uses. Local telephone companies installed more than 62,500 miles of fiber in 1984 and 100,000 miles in 1985 for their local loops (connecting telephone offices with subscriber's premises). Another 285,000 miles of fiber were installed by the same companies during those years for interoffice trunking (table 2).

Fiber optics is attractive, in part, because much higher data rates can be transmitted—about 1 gigabit per second currently—than using copper wire. One small cable containing two glass fibers can carry more than 15,000 two-way voice telephone conversations, or the

Table 2.—Telephone Company Fiber Applications
(fiber miles in thousands)

Company	1984 Long distance	1984 Loop	1985 Long distance	1985 Loop
NYNEX	25	15	50	25
Bell Atlantic	20	15	30	25
BellSouth	20	35	60	30
Ameritech	25	15	40	35
SW Bell	10	5	50	15
U.S. West	15	5	30	10
Pacific Telephone	20	15	40	25
Independents	10	—	10	5
Total	145	105	310	170

SOURCE: Annual Reports/Internal Siecor Estimates

equivalent in data signals, for up to 25 miles without requiring repeaters (amplifiers). Conventional telephone cables composed of 24 gauge copper wires, in contrast, would require 1,250 pairs of wires and repeaters spaced about 1 mile apart in order to carry the same traffic. Further advances in fiber technology are widely expected. Fiber optics also is less expensive than conventional cable, does not radiate energy under normal operating conditions, and is not as readily subject to passive or active interception as are radio signals or signals on copper wire. Figure 5 illustrates a typical fiber optic system.

Satellite Communications Systems

Satellites were first used for commercial telecommunications in the mid-1970s. Today, there are more than 100 satellites worldwide, with some two dozen providing domestic services for the United States. Still, satellites account for only a small portion of domestic transmission capacity. In terms of domestic nonbroadcast channel capacity, they are being outpaced rapidly by fiber optic cable. International communications services have, for the past decade, been provided about equally by satellite and cable facilities. This balance is likely to shift sharply with the planned use of fiber optic cable for trans-Atlantic service beginning in 1988 and for trans-Pacific service in 1989.

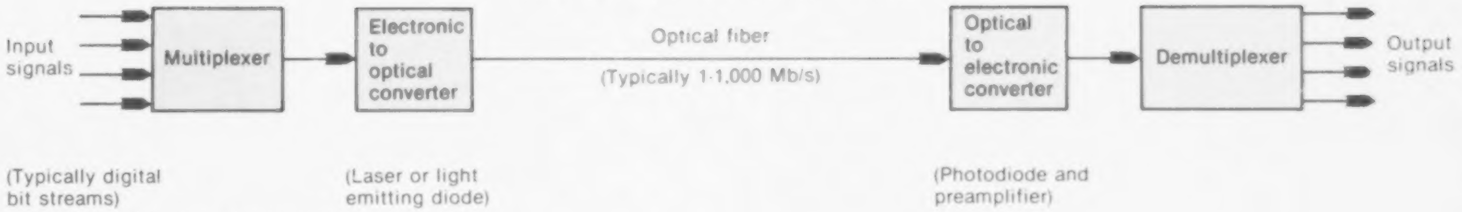
Satellite communications systems operate in much the same manner as microwave relay systems, except that the repeater or amplifier is in geostationary orbit 22,300 miles above the equator. Satellites accept signals from transmitting earth stations (the uplink), translate the signal to a different frequency band, and retransmit it at suitable power levels to receiving earth stations (the downlink).

Some satellite networks are widely used for one-way distribution services, including cable and network television, and a variety of data services, such as financial information and weather reports. Two-way distribution services include point-of-sale transactions, database inquiries, and inventory control. Most of these applications use digital transmission and various techniques to share the satellite bandwidth among the users.

The satellite "footprint," defined by the beamwidth of the spacecraft antenna, may be contoured to the shape of the intended coverage area, but is nevertheless likely to be thousands of miles across. The satellite channel is "visible" to all points within the coverage area and, therefore, readily interceptable within that area. The signals from many satellites may be received from locations beyond the borders of the contiguous United States. The key to targeted interception, consequently, is determining which satellite and transponder channel frequencies are of interest.

One of the simplest methods for intercepting subscription satellite signals was advertised until recently in an amateur radio publication and sold for less than $100. The device used a short piece of wire, cut to the proper

Figure 5.—Typical Fiber Optic System


Input signals
Multiplexer
Electronic to optical converter
Optical fiber
(Typically 1-1,000 Mb/s)
Optical to electronic converter
Demultiplexer
Output signals
(Typically digital bit streams)
(Laser or light emitting diode)
(Photodiode and preamplifier)

SOURCE: Office of Technology Assessment, 1987.

length for reception at the selected broadcasting frequency, and mounted in an ordinary metal coffee can. This apparatus was connected, through the printed circuit card provided, to the lead-in wires of a television set. All that remained was to point the coffee can at the desired satellite, adjusting by trial and error until an adequate signal was received.

These characteristics make communications satellites vulnerable to several different types of misuse. The uplinks can be overpowered by unauthorized users, whether intentionally or not, who transmit stronger signals than those used on the authorized uplink. This was the case in both of the April 1986 takeovers of the Home Box Office (HBO) channel in which a part-time satellite uplink operator and retailer of home receiving dishes overpowered the HBO uplink transmitter signal with an unauthorized one and put his own message on the screens of some 8 million viewers.[13] In addition, the downlinks can be jammed by bogus earth transmitters.

Other vulnerable parts of communications satellites include the transponders, whose lifetimes can be severely shortened by excessive received signal strength and unprotected telemetry systems, which might be manipulated to move the satellite out of its intended orbit.[14] Broadcasters and communications carriers are especially concerned about jamming since the former could lose millions of dollars if advertisements are interfered with and the latter could lose many tens of millions of dollars if a satellite's lifetime is prematurely shortened. Both groups, therefore, want to shift to a less vulnerable transmission system, such as fiber optic cable, if capacity expands sufficiently.[15] There are also concerns about the survivability of satellite communications systems in times of national emergency.[16]

Mobile Radio and Cordless Telephone Systems

Land mobile telephone service typically provides two-way, voice-grade communications between a base station and mobile units or between two mobile units. The mobile unit is most commonly a car phone, although some "briefcase phones" have recently appeared on the market. The use of these systems is growing by about 20 percent annually. In addition, one-way paging services have become very popular recently.

The antennas for these units transmit omnidirectionally. Cellular mobile systems use a base station in each cell to communicate with all mobile units within that cell. A relatively small number of frequencies are needed for each cell. Inexpensive scanners can be used to monitor for mobile call signals and to tune in to the next call made. Each call transmitted from the base station is addressed to a particular mobile unit within the cell, making targeted, passive eavesdropping simple as long as the eavesdropper knows the telephone number of interest and the cell the target is in.

Cordless telephones substitute a duplex (two-way), low-power radio link for what otherwise would be a very long extension cord. Their growing popularity and the relatively small number of channels available have created problems for some users. A cordless phone always uses the same channel in the same small area; thus, these phones are much easier to target by eavesdroppers. Nearby users with the same frequency channel pair can listen to their neighbors' calls simply by listening with their own cordless units. In addition, some people have intentionally used their remote units to initiate calls by triggering other parties' base units, thus avoiding having to pay for the call since the related bill (usually for a long-distance call) is sent to the base unit owner. This "theft of dial tone" is possible when the base unit does not have appropriate security features.[17]

---

[13] For a detailed review, see Donald Goldberg, "Captain Midnight, HBO, and World War 3," *Mother Jones*, October 1986, p. 26.

[14] The range of vulnerabilities of commercial communications satellites were discussed in some detail by representatives from HBO, CBS Technology Center, and MA-COM, Inc., at a seminar at the Massachusetts Institute of Technology on Oct. 16, 1986. Also discussed were a number of safeguards that are being considered for current and, especially, future satellites.

[15] Ibid.

[16] See "Commercial Satellite Communications Survivability Report," prepared for the National Security Telecommunication Advisory Committee (NSTAC), May 20, 1983. This report notes that:

> . . . commercial satellite communications systems are vulnerable to hostile actions which would deny service in emergency situations, particularly actions by a relatively unsophisticated antagonist—the so called "cheap shot" attack. For example, today's satellite command links provide only modest protection against electronic intrusion. Also, in nuclear war, some of the control facilities of satellite systems would become unusable.

Mobile and cordless radio have much in common, but two main differences involve signal range and the ease with which an adversary may target on particular users. Although cordless phones are easy to target, their range is typically no more than 1,000 feet, while conventional mobile radio signals may be received at a distance of 20 to 30 miles. Newer cellular mobile phones have a smaller range and use a variety of channels and base stations as they move from cell to cell, making them slightly harder to pinpoint.

Other System Components

Switching Systems

In addition to the transmission paths that connect end users and network nodes, and the network nodes to each other, switching systems located at the network nodes provide opportunities for misuse. Thousands of communications lines are concentrated at these nodes. With the use of telephone company records, individual circuits assigned to particular customers can be identified. In order to reduce opportunities for potential misuse of these records, the operating companies must carefully limit both physical and remote access to these nodes. The necessary precautions are the same as those described below in connection with the security of computer systems.

Most electromechanical switching systems require frequent maintenance, particularly those that serve large numbers of customers. On the other hand, stored, program-controlled switching systems of comparable size require less frequent onsite maintenance since many of their functions can be controlled electronically from remote, centrally located maintenance sites. From these sites, however, access can be gained to an even greater number of communications channels. This is an important reason for controlling both physical and remote access to these nodes. A special concern is electronic access to the processor used to control these switching systems: A knowledgeable individual, for example, could sabotage or manipulate the switching system (e.g., by rerouting calls destined for one person to another) without physical access to the switching systems.

Switching systems are equipped with circuitry designed to permit operators to verify that busy lines are actually in use and, in an emergency, to interrupt ongoing conversations. By the very nature of the circuitry's design, it would permit monitoring of conversations if protections were not incorporated. In fact, current versions of this circuitry have scramblers built in and, if interruption is required, periodic audible tone bursts are used to alert the users that a third party has joined their conversation.

Signaling Elements

Signaling is another element of communications systems that may provide opportunities for abuse. Signaling is normally used to send the destination address data between switching network nodes. There are signaling methods that use either slowly pulsed direct current or voice band tones that are in predominant use between customers' premises and the local telephone office.[18] These are used for voice and a substantial number of data communications. Both of these signaling methods can be monitored, using methods described above for monitoring communications, allowing an eavesdropper to intercept not only message content but also its destination.

Carriers use pen registers and modern dialed number recorders to monitor destination address signals. A new type of digitally coded address signaling is now used in connection with some data communications networks, such as packet networks. This type of signaling is also used for internode signaling in AT&T's common channel interoffice signaling system (CCIS) and some other networks. Separation of signaling information from message content increases the confidentiality of messages provided the eavesdropper does not have access to the signaling data. The CCIS encrypts the signaling information sent between nodes.

---

[17] See Federal Communications Commission, 'Further Notice of Proposed Rulemaking," Docket 83-325, released May 23, 1984.

[18] Some data communications only use these signaling methods to direct a call through the telephone network to a packet switched network and thus information about the destination address is of limited value to an adversary.

Operational Support Systems

In addition to the transmission, switching, and signaling components, communications systems include supporting equipment for testing, repairing, and maintaining customer records. The information stored in these systems could be valuable to a person seeking to intercept communications. Access to this information can be limited by time of day, terminal location or function, physical access, logon identification passwords, authorization verification, and audit trail records.

A testing system is another type of operational support system. Testing systems can gain access to specific trunk and line circuits, and thus provide an opportunity to either monitor communications or obtain information regarding communication links. These systems are often protected by many of the same techniques described above.

Commercial Availability of Interception Equipment

The very technologies that make possible continued improvements in communications and computer processing also lend themselves to illicit purposes. The successful disruption of the HBO satellite broadcast in April 1986 shows that some of these systems are no better protected against such attacks than against passive interception. This may be changing as a result of the HBO experience. The satellite transponder cannot distinguish between the legitimate signal and a bogus one—it simply selects the stronger signal.[19] In the HBO case noted earlier, the "adversary" or hacker was sophisticated technically and had access to commercially available and relatively inexpensive transmitter equipment, as well as information in the public domain concerning the satellite's location and transponder frequency.

In a completely different part of the network, wiretapping of telephone lines remains one of the simplest forms of eavesdropping, as long as physical access to wire closets and other interconnection points are generally accessible.[20] Certain types of wiretaps cannot be detected by electronic means, and some wiretaps can be performed using equipment costing as little as $12.[21] A wiretap is sufficiently easy to install that even a 9-year-old can do it.[22] Rooftop terminal junction boxes and residential junction boxes are often readily accessible to potential wiretappers. In contrast, when fiber optic cable is used to connect the user's premises to the carrier's facility (the local loop), tapping the fiber cable requires more sophisticated and expensive equipment and skill.

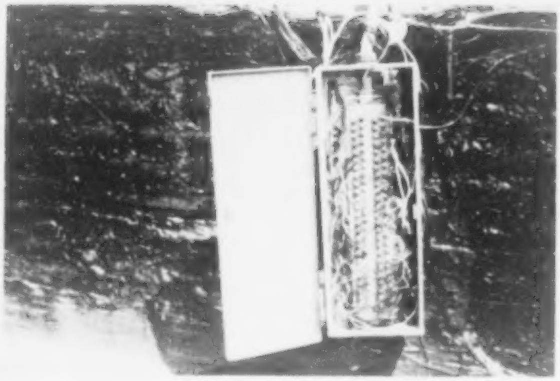
---

[19] "Mystery Broadcast Overpowers HBO," Institute for Electrical and Electronics Engineers, *THE INSTITUTE*, vol. 10, No. 10, October 1986, p. 1.

[20] In one of the relatively few examples in which telephone taps are uncovered, a tap and electronic bugging equipment were recently reported discovered in the office of the governor of New Mexico. "Capitol Bug Found," *Washington Post*, Jan. 10, 1987, p. A8.

[21] Ross Engineering Associates, "Telephone Taps," OTA contractor report, November 1986.

[22] Ibid.



Rooftop Terminal Junction Box

Photo credits: Courtesy of Ross Engineering, Adamstown, MD

Residential Junction Box

VULNERABILITIES OF COMPUTER SYSTEMS[23]

Background

In a simplified form, computer security is the ability of ensuring that people use information systems only as they are supposed to. This involves protecting:

- the system itself against failures, whether caused by deliberate misuse, human error, or technical problems; and
- the information in the system to ensure that it is seen and used only by those who are authorized to do so and that it is not accidentally or maliciously disclosed or modified.

Computer "hackers" aside, it is even more important to recognize that information security is much broader than just protection against those who would penetrate information systems from the outside. People within organizations are perhaps even more likely to misuse information systems, including unauthorized actions by those who are authorized to use the system. In addition, technical failures can be caused by natural disasters.

The rapid evolution of computer technology, and society's growing dependence on it, have important implications for information security. Three distinct kinds of technical trends can be identified that have security implications—the growth of large-scale computers, the evolution of microcomputers, and changes in computer software.

Large-Scale Computers

Advances in large-scale computing have dramatically lowered the cost of computation.[24] The power of machines relative to their cost and size has been increasing during the last 30 years by more than a factor of 10 per decade and is likely to continue increasing for the foreseeable future. These changes have been complemented by magnetic (and more recently optical) disks that can hold greater and greater amounts of information on each disk. Communication between computers has also become considerably more pervasive and efficient—line speeds are higher, protocols and technical standards have been established, and communications systems are generally evolving from analog links to digital technology.

---

[23] Because this report emphasizes telecommunications security, the treatment of computer security is brief. For more information on computer security, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Government Oversight*, OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986).

[24] In this analysis, a "large-scale" computer generally means a machine that is intended to serve multiple users performing different tasks at the same time, that is generally not considered to be a "desk-top" or "personal" computer, and that stores data on large-scale magnetic (or optical) disks rather than floppy disks or small, hard disk drives.

These increasingly powerful machines have also become much more pervasive in society. Figure 6 shows that the number of mainframe computers operated by the Federal Government has increased from about 11,000 in 1980 to 27,000 in 1985, with most of the increase coming in the Department of Defense. Perhaps more important, figure 7 shows that the points of access to Federal computers have increased geometrically in recent years, from roughly 36,000 terminals in 1980 to 173,000 terminals in 1985. Table 3 indicates similar trends in sales of large-scale host computers in the United States from 36 units in 1965 to more than 1,600 in 1985.

These trends—increased power and use of large-scale computers—have strong implications for security. First of all, the changes have resulted in increased dependence on information technology generally. That means that virtually all Government agencies and private organizations are more susceptible to technical sabotage or failure of their computers. But it also means that there is more information stored in computers, that this information is often accessible to more people, and that this information is accessible at a distance via telecommunications linkages.

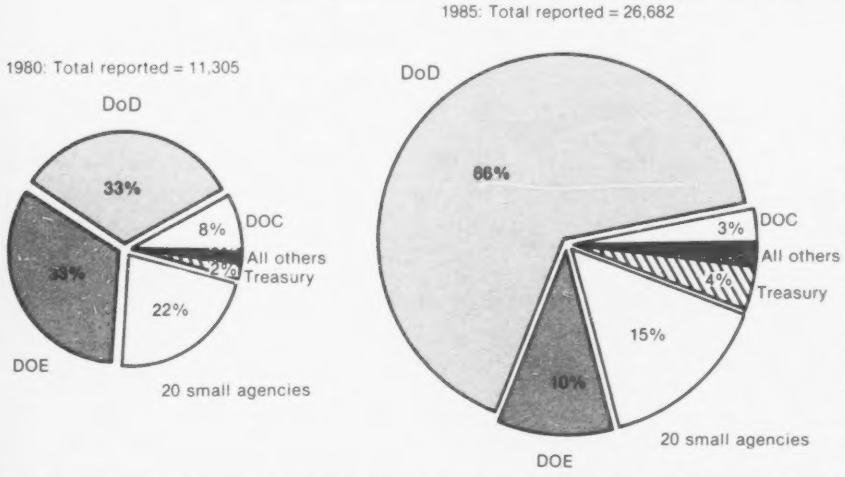
Table 3.—Sales of Large-Scale Host Computers in the United States

Year	Units	Value
1965	36	$200 million
1976	514	$ 2.2 billion
1977	611	$ 2.4 billion
1978	1,009	$ 3.9 billion
1979	1,461	$ 5.3 billion
1980	1,328	$ 4.8 billion
1981	887	$ 3.9 billion
1982	1,448	$ 6.8 billion
1983	1,836	$ 8.1 billion
1984	2,420	$ 9.0 billion
1985	1,617	$ 9.3 billion
1986 (estimated)	1,800	$ 9.7 billion
1987 (estimated)	2,090	$10.2 billion
1988 (estimated)	2,070	$10.6 billion
1989 (estimated)	2,200	$11.5 billion
1990 (estimated)	2,300	$12.1 billion

NOTE: Large-scale host computers are those machines serving more than 128 users in a normal commercial environment. This definition is not necessarily the same as that used in figure 6.

SOURCE: International Data Corp.

Figure 6.—Mainframe Computers in Federal Agencies



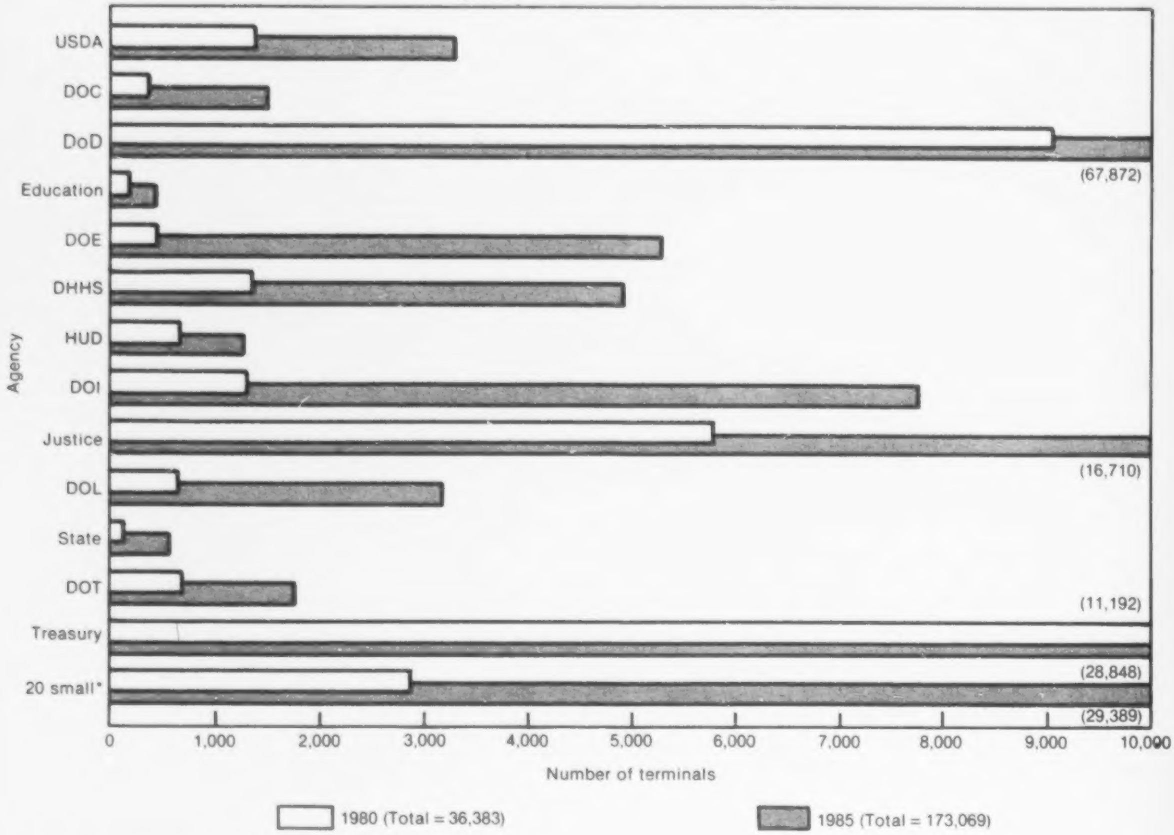
Reported numbers of mainframe computers in Federal agencies

Agency	1980	1985
USDA	13	23
DOC	967	915
DoD	3,765	17,565
Education	3	6
DOE	3,718	2,781
DHHS	48	106
HUD	3	7
DOI	81	250
Justice	28	75
DOL	11	15
State	5	6
DOT	16	15
Treasury	205	1,030
20 small agencies	2,443	3,888
Total	11,305	26,682

NOTE: Consistency in definitions of "mainframe" central processing units cannot be assured because of different interpretations of the term. Definitions may not agree with definition of large host computers in table 3.

SOURCE: OTA Federal Agency Data Request.

Figure 7.—Computer Terminals in Federal Agencies



*20 selected independent agencies that received OTA's data request.

SOURCE: OTA Federal Agency Data Request.

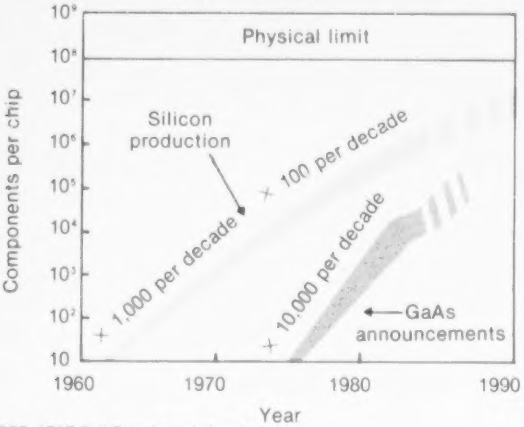
On the other hand, the increased power and sophistication of large-scale computers also means that more sophisticated safeguards are more practical than they were with smaller computers. These safeguards include "audit" programs that log the actions of each user and more powerful access controls. These and other safeguards are discussed in chapter 4.

Microcomputers

Changes in smaller desk-top or personal computers have been even more striking and rapid than those in large-scale machines. Since the first microcomputer was commercially produced in the mid-1970s, these devices have progressed to a point where their speed and power nearly equal that of mainframe computers a decade ago. These improvements are largely due to the increasing number of circuits that manufacturers can put on a single microprocessor chip. Figure 8 shows the geometric increases in the complexity of these chips, which has led to a declining cost per unit of computing power.

Microcomputers have also changed from an obscure hobbyist item to a standard and necessary piece of equipment in many homes, businesses, and Government offices. Figure 9 shows that the number of microcomputers in the Federal Government rose from only a few thousand in 1980 to about 100,000 in 1985. Ta-

Figure 8.—Trends in Component Density, Silicon Production, and Gallium Arsenide Announcements, 1960 to 1990



SOURCE: AT&T Bell Telephone Laboratories

Table 4.—Sales of Personal Computers in the United States

Year	Units (thousands)	Value (billions of dollars)
1980	379	1.1
1981	644	1.9
1982	2,884	4.2
1983	5,872	8.7
1984	6,586	13.0
1985	5,689	13.3
1986 (estimated)	6,633	14.6
1987 (estimated)	7,414	15.9
1988 (estimated)	8,262	17.7
1989 (estimated)	9,317	19.8
1990 (estimated)	10,120	21.6

SOURCE: International Data Corp.

ble 4 shows comparable trends in the Nation as a whole, with sales of personal computers rising from 380,000 in 1980 to almost 6 million in 1985.

Microcomputers are computers in their own right and thus require appropriate administrative and technical security measures to safeguard the information they process. Also, microcomputers can be networked and/or function as "smart" terminals to larger computer systems. Thus, the rapid proliferation of microcomputers cannot only place computing power in the hands of an increasing number of computer-literate individuals, but also can decentralize data processing capabilities. For example, employees of many firms or Government agencies are able to collect and manipulate information on their own desk-top microcomputers. Additionally, they are to able use these microcomputers to copy or "download" large amounts of information from the organization's central computer and also to "upload" information they have collected or manipulated into the central computer files.

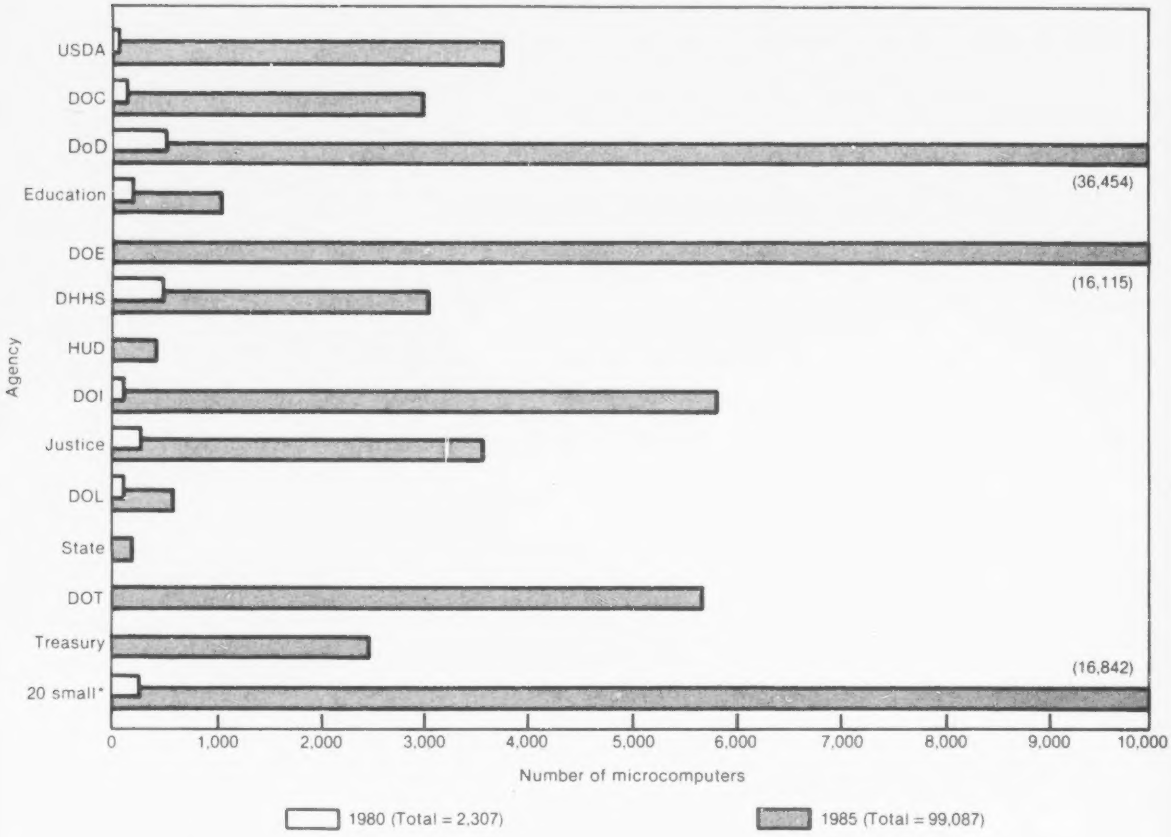
The expanding use of microcomputers can have an adverse effect on security if the appropriate security policies, procedures, and practices are not in effect. For instance, in a computer system that is not organized so as to control and monitor users' access to data files and constrain the data transactions that authorized users are permitted to perform, users can copy or manipulate data in an essentially uncontrolled fashion. There is a growing array of add-on microcomputer security products that address security problems of this sort, as well as an increasing awareness of the importance of using these safeguards. Also, the capability (at the mainframe computer) to control the downloading/uploading of data files is well within current technology. However, actual practice often falls short of the ideal, particularly in firms that do not recognize the value of electronic information in microcomputers and the importance of safeguarding it.

Using microcomputers instead of "dumb" terminals, on the other hand, can help if good security practices control the downloading and uploading of data files and if the system is configured properly. For example, data integrity can be improved by procedures requiring authorized users to make additions, corrections, or other modifications to large data files on a microcomputer. If the modified data are checked, and only then uploaded to the main computer files, then the probability of accidental or malicious deletions of main files, for instance, can be reduced.

Software

Technical sophistication in software and in databases has progressed more slowly than hardware advances. In fact, many people now

Figure 9.—Microcomputers in Federal Agencies



*20 independent agencies selected by OTA to receive the data request.

NOTE: The data request used GSA's definition of microcomputer, slightly adapted: "Any microprocessor-based workstation capable of independent use — including stand-alone and networked personal computers, professional computers, intelligent terminals, word processors, and other similar devices — costing less than $10,000 per unit, but excluding peripherals and separately purchased software."

SOURCE: OTA Federal Agency Data Request.

recognize that software is the bottleneck for many prospective applications of information technology. Nevertheless, the past two decades have seen significant increases in the size of databases that can be reasonably accommodated by software and in the sophistication of the software itself. This means, for example, that software can link disparate pieces of information in a database more readily and that users can make inquiries of databases using more natural commands.

These changes give more people direct access to computerized data and the databases contain far more information that is subject to both authorized and unauthorized use. Further, although not a subject of significant concern to many users, some security experts consider that the inferential ability to link pieces of information in a database or from different databases can have subtle but important implications for security. To date, most attention to this type of problem has been on the part of the defense and intelligence communities, but the problem can be more general. Even when the most sensitive information is unavailable, an adversary can infer critical data by combining pieces of apparently innocuous information (e.g., determining information about the design of a company's product from its orders for raw materials).

The Extent of Computer Misuse

A variety of recent studies have indicated substantial increases in computer misuse. However, information available about the extent of computer misuse is spotty. Moreover, these studies suffer from serious shortcomings that make generalizations difficult (large successful frauds are often not reported, let alone prosecuted).

The most significant studies and findings include:

- The American Bar Association's 1984 "Report on Computer Crime." In a survey of 283 public and private sector organizations, ABA found that 25 percent of the respondents reported "known and verifiable losses due to computer crime during the last 12 months."
- The American Institute of Certified Public Accountants 1984 "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries." AICPA surveyed 5,127 banks and 1,232 insurance companies. Two percent of the banks and 3 percent of the insurance companies said they had experienced at least one case of fraud related to electronic data processing. Sixteen percent of the frauds were reported to involve more than $10,000, although that figure does not reflect funds that were recovered.
- The President's Council on Integrity and Efficiency issued "Computer-Related Fraud in Government Agencies: Perpetrator Interviews," in May 1985. The Council surveyed Federal agencies and found a total of 172 relevant cases of computer fraud or abuse. The losses in fraud cases ranged from zero to $177,383, with the highest proportion in the $10,000 to $100,000 range.
- The Department of Justice's Bureau of Justice Statistics 1986 report "Electronic Fund Transfer System Fraud." This reported a study of fraud related to the transfer of electronic funds in key banks. The study estimated that banks nationwide lost $70 million to $100 million annually from automatic teller fraud. It also examined losses from wire transfers, although there were insufficient data to estimate national loss levels. Twelve banks reported 139 wire transfer fraud incidents within the preceding 5 years, with an average net loss (after recovery efforts) per incident of $18,861. However, the loss exposure or the potential loss per wire transfer incident averaged nearly $1 million.
- *Security* magazine and the Information Systems Security Association surveyed their subscribers and members in 1985 and 1986. Eighteen percent of the 1986 respondents reported that their company had detected a computer crime in the last 5 years, compared with 13 percent reported by the 1985 respondents. The respondents rated the threats to computers, in descending order: unauthorized use by employees, routine errors and omissions, carelessness with printouts, theft of computers, fire damage, use/misuse by outsiders, and vandalism.

While these studies are far from conclusive, it is apparent that deliberate misuse of computers is a significant and growing problem.

TYPICAL VULNERABILITIES OF INFORMATION SYSTEMS

The combined advances in communications and computer technologies have resulted in information systems that are an order of magnitude more complex than those of 10 or 20 years ago. Not only is computing power greatly increased, but it is also more decentralized—and communication between computers and interconnected devices has become far more pervasive. In some ways, this has improved security in that, for example, information is no longer stored in just one large computer, which could result in chaos if it failed. On the other hand, information systems are much more extensively linked and interdependent, and the number of points from which technical failure, deliberate misuse, or accidental errors could cause serious problems has increased geometrically.

To illustrate the numerous vulnerabilities of computer systems, figure 10 presents a schematic diagram of a typical information system. The circled letters in the figure correspond to certain types of vulnerabilities (discussed below) that encompass the vast majority of potential problems caused by deliberate misuse of computer systems. Some problems are more important in some systems than in others and potential adversaries may be more or less sophisticated. As will be seen in chapter 4, good security practices would require security officials to perform an analysis of each system to determine which vulnerabilities and threats are most significant and what protective measures would be most appropriate and cost-effective.

The first two kinds of vulnerabilities do not require direct on-line access to data and, generally, an adversary needs relatively few resources to exploit them. The first (a) is theft of storage media that contains valuable data. Theft (or copying) of personal computer diskettes, for example, can be particularly easy because personal computer users often do not lock up their diskettes. Similarly, theft of printouts (b), especially discarded ones, is typically quite easy and has been the source of a significant amount of computer abuse. The printouts may contain valuable competitive information or account and password information that allows an unauthorized person to later gain electronic access to the system.

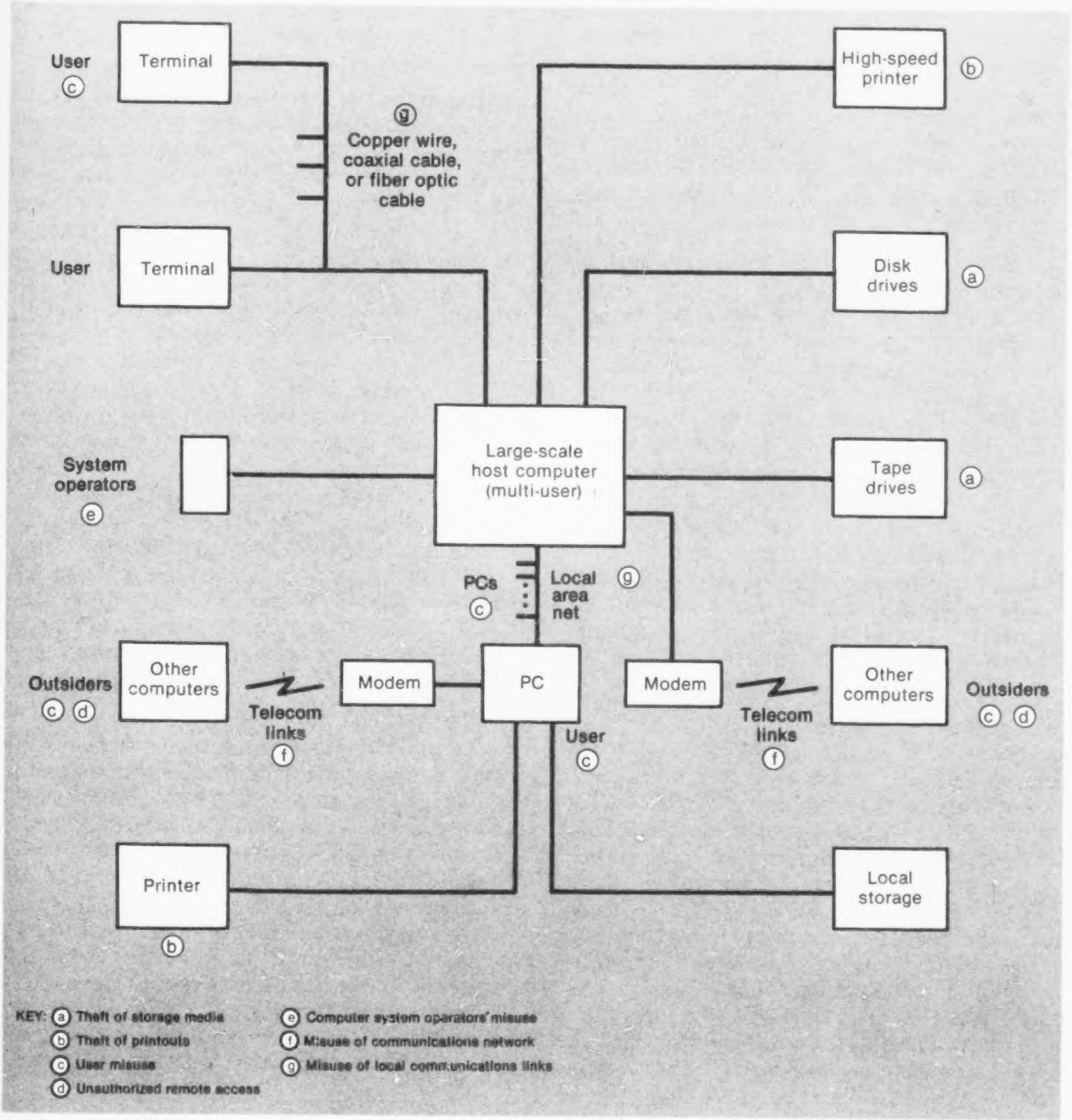
The next type of vulnerability is misuse of computer systems by those who are authorized to use them (c). The misuse can consist, for example, of stealing corporate secrets, changing personnel information, causing falsified checks to be written, or damaging databases. This type of misuse typically requires only a moderate level of sophistication on the part of the perpetrator, although in some cases (e.g., falsified disbursements) it requires collusion between two or more workers.

Moving up one step further in level of adversary, outsiders who gain unauthorized access to a computer system can perpetrate the same kinds of misuse. This usually requires covertly obtaining an account name and password by, for example, looking over the shoulder of an authorized user, finding a discarded computer printout, using codes written on cards or pieces of paper taped to the terminal, or simply guessing. Such an outsider could either seek to gain access to an authorized user's local terminal or personal computer (c) or could try to access the system from a remote location via phone lines (d). Access via phone lines is inherently less risky for the perpetrator since it is often less protected by security measures than local access. The dangers of hobbyists prowling in computers via phone lines are often overstated compared with misuse by those authorized to use computer systems. However, it is likely that long-distance computer abuse will continue to grow and more serious adversaries (e.g., technically adept criminals, including organized crime) will be involved.

Computer system operators (e), such as programmers and managers, sometimes have access to user passwords. Although this is becoming less common, they still generally have access to stored files unavailable to other users. In particular, programmers have the technical expertise to perpetrate sophisticated sabotage and misuse, including such exotic attacks as "logic bombs" that render a system unusable after a specified period of time or at a specific time (often after the disgruntled programmer is no longer employed at the site).

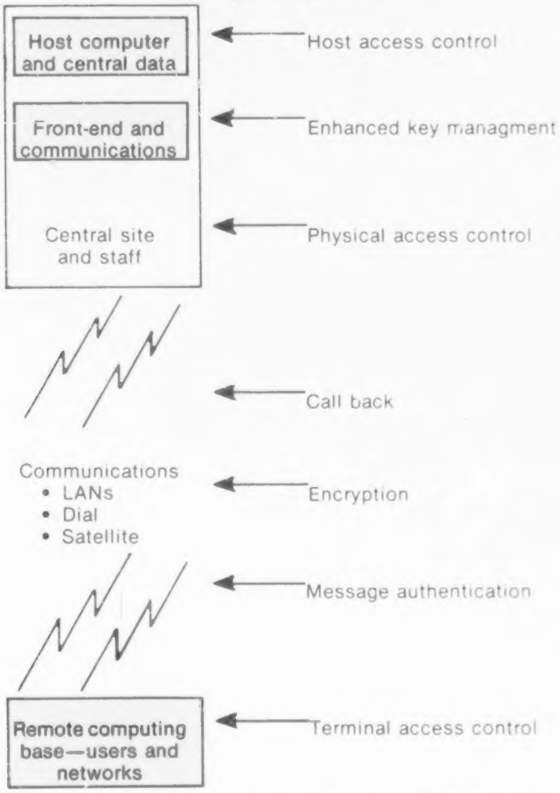
The last two vulnerabilities, eavesdropping on computer transmissions through either telecommunications links (f) or local connections (g), are discussed in previous sections of this chapter. Chapter 4 describes some of the safeguards that have been developed to address these vulnerabilities and prevent such crimes in the future. Figure 11 shows how these safeguards can be used in computer networks.

Figure 10.—Typical Vulnerabilities of Computer Systems



SOURCE: Office of Technology Assessment, 1987

Figure 11.—Technical Safeguards for Computer Systems



SOURCE: *Personal Identification News* (Washington, DC: Warfel & Miller, Inc. 1986).

Chapter 4

Security Safeguards and Practices

CONTENTS

Page
Findings . . . 51
Introduction . . . 51
Encryption . . . 54
  Encryption Algorithms . . . 54
  Message Authentication . . . 59
  Public-Key Ciphers . . . 61
  Digital Signatures . . . 63
New Technologies for Private and Secure Transactions . . . 68
Key Management . . . 69
Voice and Data Communications Encryption Devices . . . 71
Personal Identification and User Verification . . . 72
  Background . . . 72
  Conventional Access Controls . . . 73
  Biometric and Behavioral Identification Systems . . . 77
Access Control Software and Audit Trails . . . 83
  Host Access Control Software . . . 83
  Audit Trails . . . 86
Administrative and Procedural Measures . . . 86
Computer Architectures . . . 88
Communications Linkage Safeguards . . . 89
  Port-Protection Devices . . . 89
  Satellite Safeguards . . . 90
  Fiber Optic Communications . . . 90
  Common Carrier Protected Services . . . 90

Boxes

Box *Page*
B. An Example of DES Encryption . . . 57
C. Application of Message Authentication to Electronic Funds Transfer . . . 60
D. Host Access Control Software . . . 84

Figures

Figure No. *Page*
12. Common Administrative, Physical, and Technical Information Security Measures . . . 52
13. DES Encryption in Electronic Codebook Mode . . . 56
14. Federal Standard for Authentication . . . 62
15. Public-Key Ciphers . . . 64
16. Digital Signatures Using a Public-Key Cipher . . . 66
17. A Description of the Past Network Environment . . . 74
18. A Description of the Current/Future Network Development . . . 75
19. The Mechanics of See-Through Security . . . 76
20. Biometric Identification Configuration Alternatives: Host-Based v. Stand-Alone . . . 78
21. Example Reports From Audit Trail Software . . . 87

Tables

Table No. *Page*
5. Major Characteristics of Automated Biometric Identification Types . . . 79
6. Configurations and Applications of Biometric Devices . . . 80

Chapter 4

Security Safeguards and Practices

FINDINGS

- **Technical safeguards for computer and communications systems are still evolving, as are users' understanding of their needs for them. Products and systems are available for controlling access and auditing use and for encrypting data.**
- **Technical safeguards alone cannot protect information systems completely. Effective information security requires an integrated set of safeguard technologies, management policies, and administrative procedures.**
- **Information security hinges on the security of each segment of the increasingly intertwined computer and communications network.**
- **A number of important techniques are emerging to verify the identities of the senders of messages, authenticate their accuracy, and ensure confidentiality. Mathematical techniques using cryptography cannot only provide improved information security, but also broaden the applicability of electronic transactions in commerce.**
- **The Federal Government has played an important role in promoting technical standards for selected information safeguards, particularly for cryptography. Yet, the public position of the Government in general and the National Security Agency, in particular, has been inconsistent. This inconsistency is especially apparent in providing Federal leadership for the development of information security standards; e.g., in NSA's reversal of endorsements of an open encryption algorithm and of dependence on consensus agreement in developing encryption-based security standards.**
- **Questions are being raised about the efficacy of the NSA's developing unified sets of standards and guidelines for government-wide and private nondefense use.**

INTRODUCTION

Technology that can help promote information security can be divided into administrative, physical, and technical measures. Figure 12, which shows examples of each of these categories, demonstrates the diversity of safeguard applications and the range of approaches to improved safeguards.[1]

Like the range of threats and vulnerabilities that afflict different information systems, there is a wide range of safeguards that can help protect them. Although administrative and procedural measures are also fundamentally important to good overall security, this chapter concentrates primarily on technical safeguards. These include the following:

- *Encryption*, which can be used to encode data prior to transmission or while stored in computers, to provide an electronic

---

[1] This section examines safeguards for both computers and communications since many of the measures discussed apply to both.

Figure 12.—Common Administrative, Physical, and Technical Information Security Measures

Administrative security measures:
- Background checks for key computer employees.
- Requiring authority of two employees for disbursements.
- Requiring that employees change passwords every few months, do not use the names of relatives or friends, and do not post their passwords in their offices.
- Removing the passwords of terminated employees quickly.
- Providing security training and awareness programs.
- Establishing backup and contingency plans for disasters, loss of telecommunications support, etc.
- Storing copies of critical data off-site.
- Designating security officers for information systems.
- Developing a security policy, including criteria for sensitivity of data.
- Providing visible upper management support for security.

Physical security measures:
- Locking up diskettes and/or the room in which microcomputers are located.
- Key locks for microcomputers, especially those with hard disk drives.
- Requiring special badges for entry to computer room.
- Protecting computer rooms from fire, water leakage, power outages.
- Not locating major computer systems near airports, loading docks, flood or earthquake zones.

Technical security measures:
- Audit programs that log activity on computer systems.
- Access control systems that allow different layers of access for different sensitivities of data.
- Encrypting data when it is stored or transmitted, or using an encryption code to authenticate electronic transactions.
- Techniques for user identification, ranging from simple ones such as magnetic stripe cards to more esoteric "biometric" techniques, which rely on hand or eye scanners (just beginning to be used).
- "Kernel"-based operating systems, which have a central core of software that is tamperproof and controls access within the system.*
- "Tempest" shielding that prevents eavesdroppers from picking up and deciphering the signals given off by electronic equipment.*

*Generally used only in military or other national security applications in the United States.

SOURCE: U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight*, OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986), p. 61.

"signature," and to verify that a message has not been tampered with.

- *Personal identification and user verification techniques*, which can help ensure that the person using a communications or computer system is the one authorized to do so and, in conjunction with *access control systems* and other security procedures, that authorized users can be held accountable for their actions.
- *Access control software* and *audit trails*, which protect information systems from unauthorized access and keep track of each user's activities.
- *Computer architectures* that have been specifically designed to enhance security.
- *Communications linkage safeguards*, which hamper unauthorized access to computers through phone lines.

The systems of safeguards that are being developed fall into categories that control access to data or monitor user activities and others that protect the integrity of data, e.g., verify its accuracy. Technology is paving the way for further improvements in these and still other categories. Systems that will combine improving message integrity with preventing unauthorized activity are beginning to set the stage for major new applications with broad commercial applications.

Security is never just a "black box" of technical safeguards that can be purchased and added to computer or communications systems. Moreover, technical measures would be fruitless unless accompanied by suitable policies and administrative procedures. For security measures to be effective, they must be planned for and managed throughout the design and operation of computer and communications systems. This chapter, however, mainly discusses the technology of safeguarding information systems.

In addition, for many types of users, the combination of reasonable effectiveness and convenience are more important than extremely high security. Determining which safeguards are appropriate for a particular computer or communications system requires an analysis of such factors as the value of the information at risk, the value of the system's reliability, and the cost of particular safeguards. Security experts disagree about how this "risk analysis" ought to be conducted and about the problems with, and validity of, risk analyses. But, some form of risk analysis—whether formal or informal, quantitative or qualitative—remains the chief means by which managers can assess their needs and evaluate the costs and benefits of various security measures.

The National Bureau of Standards (NBS) has played an important role in developing computer security standards. This role has become complicated by the recent entry of the NSA into the standards arena and by NSA's efforts to develop comprehensive standards suitable for all users' needs.

There are four driving forces behind the emergence of the new safeguard technologies:

1. developments in microelectronics and information processing, such as smart cards and other hardware implementing encryption algorithms;
2. developments in cryptography, such as asymmetric and public-key ciphers;
3. developments in the mathematics underlying signal processing and cryptography; and
4. developments in software, particularly for processing biometric personal identification data.

A number of technologies exist that can verify that individual users are who they claim to be. Similarly, technologies exist to authenticate the integrity of a message and to ensure its confidentiality. These developments are being applied mainly to solve some of today's problems concerning information security.

Technologies for user verification, often intended for use in conjunction with other access control systems, include: hand-held password generators, "smart" key cards with embedded microprocessors, and a number of personal identification systems based either on biometric measurements or other individual characteristics. Message authentication techniques rely on combinations of encrypting and/or "hashing" schemes to create a code authenticating the accuracy of a message's content. A variation of this technique can provide a "digital signature" that not only authenticates the message, but also establishes the identity of its sender. Encryption methods are widely available to protect against unauthorized disclosure of messages.

What is becoming increasingly apparent, however, is that some of this same technology has far greater potential uses. One of the central observations of this chapter is that measures, particularly technical measures, are beginning to be developed that provide some of the tools likely to prove important in the long term for more secure operation of electronic information systems in uncontrolled, even hostile environments. These include environments, such as the public switched telephone network for example, where sensitive data is unavoidably exposed to risks of being improperly accessed, modified, or substituted, or where errors can be introduced by the system itself, as from normal electronic noise in communications systems. Information security technology shows promise for greatly expanding the range of applications of computer and communications systems for commerce and society. It will accomplish this by reducing the cost of many of today's paper-based business transactions, by providing legally binding contracts executed electronically, and by protecting intellectual property and the privacy of personal data stored in electronic form. (See ch. 5.)

To achieve most of the above, cryptography is critically important. There are no close substitutes for cryptography available today. Cryptography, however, is a technology in which the Government has acted somewhat inconsistently by controlling private sector activity in some ways, while occasionally stimulating it in others. Thus, the technology that is important to future applications of information security is coupled to Federal policies that can encourage or inhibit its advancement. Options for the future role of Federal policies in influencing technological developments are discussed in chapter 7.

There are two principal uncertainties in the future development of safeguards. The first is the extent to which users of computer and communications systems will, in fact, buy and use the safeguards that are available. Some of the key factors that will influence users' actions include their evolving awareness of threats and vulnerabilities, the practices of their insurance companies, the evolution of "standards of due care" related to security practices, the Federal role as a leader and shaper of the field, and news media attention to incidents of misuse. Information and communication system risk analyses, based on historical threat and vulnerability profiles, will influence the marketplace for safeguards. If the demand for safeguards increases, then the market will no doubt respond with more products and techniques. On the other hand, if many users' interest in security levels off, there may be a shakeout in the market for safeguard devices, perhaps leaving mainly those products developed for Government agencies.

The second major uncertainty is the extent to which vendors of these safeguards, in collaboration with users, will be able to develop systems that use multiple safeguards in a simple, integrated fashion. If demand for safeguards becomes a significant fraction of the overall computer and communications system market, the resulting products are more likely to be well integrated, easy to use, and low cost. For someone who needs to gain access to his or her company's mainframe computer from home, for example, appropriate safeguards might include the functions of a hand-held personal identification device, encryption of the telecommunications link, passwords, dial-back modems, and audit logs at both the microcomputer and the host computer. Using such a combination would be tremendously cumbersome at present, requiring multiple pieces of hardware, software, and passwords. Thus, a major challenge for the industry is to develop systems that allow the various safeguards to work together and to become virtually invisible to the user, as well as cost-effective.

ENCRYPTION

Encryption is the most important technique for improving communications security. It is also one of several key tools for improving computer security. Good-quality encryption is the only relatively sure way to prevent many kinds of deliberate misuse in increasingly complex communications and computer systems with many access points. Of course, encryption is not a panacea for information security problems. It must be used in concert with other technical and administrative measures, as described below. In particular, effective key management is crucial.

Encryption Algorithms

The various techniques for encrypting messages, based on mathematical algorithms, vary widely in their degree of security. The choice of algorithms and the method of their development have, in fact, been among the most controversial issues in communications and computer security. (See ch. 6.) The various algorithms currently available differ along the following dimensions:

- *The mathematical sophistication and computational complexity of the algorithm itself.*—More complex algorithms may be (though not necessarily) harder for an adversary to decrypt or break.
- *Whether the algorithm is for a symmetric cipher or an asymmetric one.*—Symmetric ciphers use the same key for encryption and decryption, while asymmetric ciphers use different but related keys.
- *The length of the key used to encrypt and decrypt the message.*—Each algorithm uses a series of numbers known as a key that can change with each message, with each user, or according to a fixed schedule. Generally, for an algorithm of a given complexity, longer keys are more secure. One of the important factors in selecting keys is to make sure that they cannot be easily guessed (e.g., using a phone number) and that they are as random as possible (so that an adversary cannot determine a pattern linking all the keys if one is discovered).
- *Whether the algorithm is implemented in software (programming) or hardware (built*

into an integrated circuit chip).—Hardware tends to be much faster than software, although less versatile and portable from one machine to another.

- *Whether the algorithm is open to public scrutiny.*—Some nongovernment experts argue that users have more confidence in an algorithm if it is publicly known and subject to testing. NSA and others, on the other hand, assert that the algorithm is one of three essential pieces of information an adversary must have to decrypt a message (along with the key and access to the message itself) and that secret algorithms are thus more secure.[2] A related argument is that if an algorithm is publicly known, standardized, and widely used, it becomes a more attractive target for cracking than algorithms that are seldom used. The Data Encryption Standard (DES, see below) is one of the few working algorithms that is open to public scrutiny. Most of the other privately developed and all of the NSA-developed algorithms currently in use have been kept secret.

DES is probably the most widely known modern encryption algorithm. (See app. C for background on its development.) Based on an algorithm developed by IBM, DES was issued as a Federal standard in 1977. Although publicly known and subject to scrutiny for more than 10 years, most experts are confident that it is secure from virtually any adversary except a foreign government. The level of security is gradually weakening, however, because of the decreasing cost of computer power and the possibility of using many computing devices in parallel to crack the algorithm.

DES has four approved modes of operation, specified in FIPS Publication 81 ("DES Modes of Operation," Dec. 2, 1980). The modes vary in their characteristics and properties. The four modes are the electronic codebook (ECB), cipher block chaining (CBC), cipher feedback (CFB), and the output feedback (OFB) modes. (See app. C.) The CBC and CFB modes can be used for message authentication. The ECB mode, the simplest to understand, is illustrated in figure 13 and box B. One property of this mode, however, is that the same plaintext will always produce identical ciphertext for a given encryption key. This characteristic makes the ECB mode less desirable, especially for repetitive messages or messages with common content (e.g., routing headers or logon identifications) because a known plaintext cryptographic attack is more easily mounted, i.e., where both the encrypted and unencrypted text are available to the cryptanalyst.

DES is a "private key" cryptographic algorithm, which means that the confidentiality of the message, under normal conditions, is based on keeping the key secret between the sender and receiver of the message. (See the section on key distribution, below.) The other principal form of algorithm is called a "public key" system, which uses two keys that are mathematically related—one that each user publishes and one that he keeps secret. Using a public key system, many people can encrypt messages sent to a particular correspondent (using his or her public key), but only that correspondent can decrypt messages because the decryption key is (in principle) kept secret. These algorithms are discussed in more detail below, and also in appendixes C and D.

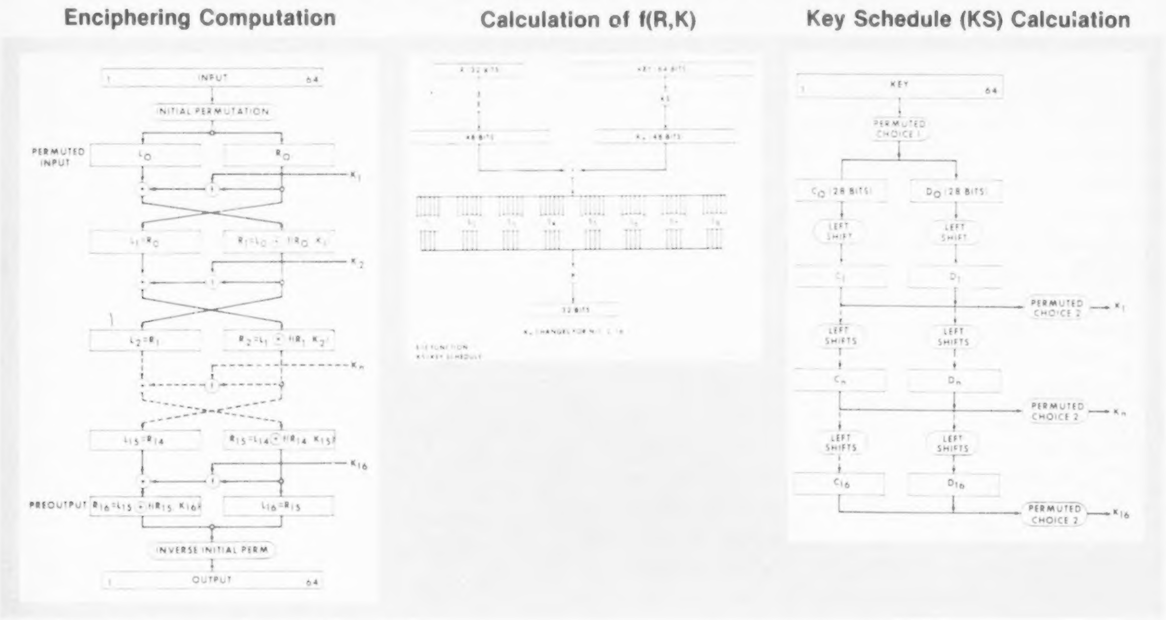
The development of encryption algorithms has been a rather idiosyncratic, scattered process, and is likely to continue to be. The academic community of cryptographic researchers is a growing and active one, although its numbers are relatively small compared to some other scientific fields.[3] Only a handful of people in the United States outside NSA have attempted seriously to create, validate, and implement new high-quality encryption algorithms. Most algorithms currently in use can be traced to the work of a few individuals. Cryptographic research requires a high level of ability in specialized areas of mathematics and/or computer science. Different skills are required

---

[2] Ted Goeltz, "Why Not DES?" *Computers and Security*, vol. 5, March 1986, pp. 24-27.

[3] R. Rivest, Massachusetts Institute of Technology, personal communication with OTA staff, Feb. 4, 1987.

Figure 13.—DES Encryption in Electronic Codebook Mode


Enciphering Computation

Calculation of f(R,K)

Key Schedule (KS) Calculation

SOURCE: NBS FIPS Publication 74, Apr. 1, 1981, pp. 21-23.

to develop operational safeguards than for theoretical research.

Despite the relatively small size of the scientific community, cryptography has been a controversial science. For example, there have been controversies concerning attempts by NSA to control Federal research funding as well as the publication and patenting of private sector and academic results in cryptographic research during the past decade for reasons of national security.[4] NSA does not at present have the legislated authority to require prepublication review of independent, nongovernment research.

However, following the controversy sparked in part by secrecy orders imposed in 1978 on two patent applications for cryptographic inventions, NSA, in concert with some academic researchers, instituted a voluntary review for cryptography manuscripts.[5] Through this process, researchers may submit manuscripts to NSA prior to their publication, giving NSA the opportunity to request suppression of sensitive material. Although many researchers and research institutions take part in this voluntary process, others do not, considering it a threat to the free exchange of scientific ideas.[6]

The voluntary review service is similar to the one proposed by the Public Cryptography Study Group of the American Council on Education (ACE), which was assembled in 1980 at the request of NSA. The group accepted the premise that "some information contained in cryptology manuscripts could be inimical to the national security of the United States." It recommended a voluntary rather than statutory solution to this problem.[7] However,

---

[4] Tom Ferguson, "Private Locks, Public Keys, and State Secrets: New Problems in Guarding Information with Cryptography," Harvard University Center for Information Policy Research, Program on Information Resources Policy, April 1982.

[5] U.S. Congress, House Committee on Government Operations, "The Government's Classification of Private Ideas," Thirty-Fourth Report (House Report No. 96-1540), 96th Cong., 2d sess., Dec. 22, 1980.

[6] See: "Brief U.S. Suppression of Proof Stirs Anger," *The New York Times*, Feb. 17, 1987, p. C3

[7] "Report of the Public Cryptography Study Group," *Academe*, vol. 67, December 1981, pp. 372-382.

Box B.—An Example of DES Encryption

The Electronic Codebook (ECB) mode is a basic, block, cryptographic method which transforms 64 bits of input to 64 bits of output as specified in FIPS PUB 46. The analogy to a codebook arises because the same plaintext block always produces the same ciphertext block for a given cryptographic key. Thus a list (or codebook) of plaintext blocks and corresponding ciphertext blocks theoretically could be constructed for any given key. In electronic implementation the codebook entries are calculated each time for the plaintext to be encrypted and, inversely, for the ciphertext to be decrypted.

Since each bit of an ECB output block is a complex function of all 64 bits of the input block and all 56 independent (non-parity) bits of the cryptographic key, a single bit error in either a ciphertext block or the non-parity key bits used for decryption will cause the decrypted plaintext block to have an average error rate of 50 percent. However, an error in one ECB ciphertext block will not affect the decryption of other blocks, i.e., there is no error extension between ECB blocks.

If block boundaries are lost between encryption and decryption (e.g., a bit slip), then synchronization between the encryption and decryption operations will be lost until correct block boundaries are reestablished. The results of all decryption operations will be incorrect until this occurs.

Since the ECB mode is a 64-bit block cipher, an ECB device must encrypt data in integral multiples of 64 bits. If a user has less than 64 to encrypt, then the least significant bits of the unused portion of the input data block must be padded, e.g., filled with random or pseudo-random bits, prior to ECB encryption. The corresponding decrypting device must then discard these padding bits after decryption of the chapter text block.

The same input block always produces the same output block under a fixed key in ECB mode. If this is undesirable in a particular application, the CBC, CFB or OFB modes should be used. An example of the ECB mode is given in table B1.

Table B1.—An Example of the Electronic Codebook (ECB) Mode

The ECB mode in the encrypt state has been selected.

Cryptographic key = 0123456789abcdef

The plaintext is the ASCII code for "Now is the time for all." These seven-bit characters are written in hexadecimal notation (0,b7,b6,...,b1).

Time	Plaintext	DES input block	DES output block	Ciphertext
1	4e6f772069732074	4e6f772069732074	3fa40e8a984d4815	3fa40e8a984d4815
2	68652074696d6520	68652074696d6520	6a271787ab8883f9	6a271787ab8883f9
3	666f7220616c6c20	666f7220616c6c20	893d51ec4b563b53	893d51ec4b563b53

The ECB mode in the decrypt state has been selected.

Time	Ciphertext	DES input block	DES output block	Plaintext
1	3fa40e8a984d4815	3fa40e8a984d4815	4e6f772069732074	4e6f772069732074
2	6a271787ab8883f9	6a271787ab8883f9	68652074696d6520	68652074696d6520
3	893d51ec4b563b53	893d51ec4b563b53	666f7220616c6c20	666f7220616c6c20

SOURCE: NBS, FIPS Publication 81, Dec. 2, 1980, pp. 12-13.

some researchers, including one member of the ACE group, felt that even voluntary restraints would affect the quality and direction of basic research in computer science, engineering, and mathematics.[8]

Currently, although some researchers feel that tensions between NSA and the research community have eased, others still consider that the prospect of NSA controls may discourage researchers, particularly academics, from pursuing problems related to cryptography. The issue continues to simmer, particularly because cryptography presents some interesting mathematical problems. For example, a controversy recently arose when the U.S. Patent and Trademarks Office, at the request of the U.S. Army, placed a secrecy order—which the Army later requested be rescinded—on a patent application filed by Israel's Weizmann Institute. The patent application dealt with an area of mathematics called "zero-knowledge proof," pioneered by Silvio Micali and colleagues at the Massachusetts Institute of Technology, that is considered to hold great promise for identification procedures ranging from credit card verification to military "friend or foe" recognition signals.[9]

---

[8] "The Case Against Restraints on Nongovernmental Research in Cryptography: A Minority Report by Professor George I. Davida," *Academe*, December 1981, pp. 379-382.

Another controversy concerns NSA's decision not to recertify DES when it comes up for its 5-year review in 1987. NSA announced in 1986 that it will continue to endorse cryptographic products using DES until January 1, 1988, but not certify the DES algorithm or new DES products after that date, except for electronic funds transfer applications. However, DES equipment and products endorsed prior to January 1, 1988, may be sold and used after that date. In justifying this decision, NSA argues that DES has become too popular and widespread in use, and thus too attractive a target for adversaries seeking to crack it. Some observers have expressed concern that NSA's decision implies that DES is no longer secure. However, NSA has stated that there are no known security problems or risks involved with the continued use of DES equipment.[10]

Instead of recertifying DES, NSA plans to provide and certify three classified algorithms. The new algorithms will use tamper-protected, integrated circuit modules directly in the products of qualified vendors. This decision officially affects only U.S. Government agencies and contractors, but it may discourage others from using DES except for electronic financial transactions.[11] The NSA plans affect safeguard vendors in two major ways: first, only selected U.S. vendors will be allowed to purchase the modules for incorporation into their products, and second, classified information (and the need to handle and protect such information) will be introduced into the product design process.[12] Also, some industry sources have expressed concern that the new secret algorithms are of uncertain reliability and will likely allow NSA itself to eavesdrop on their communications.[13]

In any case, industry has certain needs, most notably for easily exportable encryption devices and software-based encryption, that the new algorithms are unlikely to meet. Many experts consider software-based encryption less secure than hardware-based encryption, in part because the key might be exposed during encryption. Also, encryption using software is much slower than that using hardware or firmware devices. Nevertheless, some private sector users prefer software because it is inexpensive and compatible with their existing equipment and operations. For instance, reader surveys conducted by *Security* magazine in 1985 and 1986 found that about half of the respondents stated that they used encryption software.[14]

To date, there are no Federal software encryption standards and NSA has stated that it will not endorse software encryption products. Also, the new encryption modules are not exportable. NSA has not yet announced whether it will provide exportable modules for use by the private sector. Thus, the NSA decision not to recertify DES has cast doubt on the reliability of the algorithm without providing a replacement that can meet the full range of users' needs. Chapter 6 discusses Federal policy in more detail.

---

[9] The invention was made by Adi Shamir, Amos Fiat, and Uriel Feige. According to press accounts, the research had previously been cleared by NSA's voluntary review process, and NSA intervened to have the secrecy order reversed. *The New York Times*, Feb. 17, 1987: "A New Approach to Protecting Secrets Is Discovered," p. C1; and "Brief U.S. Suppression of Proof Stirs Anger," p. C3.

[10] Harold E. Daniels, Jr., National Security Agency, letter N/2338 to DataPro Research Corp., Dec. 23, 1985.

[11] The Treasury Department has embarked on a major plan using DES to authenticate electronic funds transfers. For these applications, Treasury will certify the DES and DES-based equipment. See ch. 5.

[12] S. Lipner, Digital Equipment Corp., personal communication with OTA staff, Dec. 24, 1986. See ch. 5 for a description of vendor eligibility requirements.

[13] IEEE Subcommittee on Privacy, meeting at OTA, July 8, 1986.

[14] These data were reported in: Kerrigan Lyndon, "Protecting the Corporate Computer," *Security World*, Oct. 1985, pp. 35-56; and Susan A. Whitehurst, "How Business Battles Computer Crime," *Security*, October 1986, pp. 54-60. Of the 1985 survey respondents, 48 percent reported using data encryption software compared to only 19 percent reporting use of data encryption hardware. Of the 1986 respondents, 47 percent reported using encryption software; the percentage using encryption hardware was not reported.

OTA's analysis suggests that there are certain kinds of algorithms not widely available that would substantially increase the range of applications for which encryption would be useful. These include algorithms that are very fast (require little processing time), secure enough to ensure confidentiality for relatively short periods (e.g., days or months for financial transactions, as opposed to years or decades for defense and intelligence information), and easily implemented in software, especially software for microcomputers. In addition, because of the widespread acceptance of DES for unclassified information, some experts argue that it would be fruitful to develop an improved version of that algorithm that would lengthen the key while using the same essential scheme. However, the commercial market for cryptographic safeguards is still new and small, and it has thus far been dominated by DES. Although a number of firms—mostly NSA contractors or spinoffs of these—are reportedly working on new encryption algorithms and products for the commercial market,[15] as of early 1987 public-key systems are the only area of encryption algorithm development in which substantial nongovernment research and development is evident. Developing a new algorithm may take anywhere from 5 to 20 person-years, so many firms—except, perhaps, large firms that ordinarily devote such substantial resources to long-term research and development—may hesitate to invest in a new cryptographic product for a market that, so far, has been shaky.[16]

Message Authentication

An "authentic" message is one that it is not a replay of a previous message, has arrived exactly as it was sent (without errors or alterations), and comes from the stated source (not forged or falsified by an imposter or fraudulently altered by the recipient).[17] Encryption in itself does not automatically authenticate a message. It protects against passive eavesdropping automatically, but does not protect against some forms of active attack.[18] Encryption can be used to authenticate messages, however, and the DES algorithm is the most widely used cryptographic basis for message authentication.

As the use of electronic media for financial and business transactions has proliferated, message authentication techniques have evolved from simple pencil-and-paper calculations to sophisticated, dedicated hardware processors capable of handling hundreds of messages a minute. In general, the various techniques can be grouped together according to whether they are based on public or, at least in part, on secret knowledge.

Public techniques share a common weakness: they check against errors, but not against malicious modifications. Therefore, fraudulent messages might be accepted as genuine ones because they are accompanied by "proper" authentication parameters, based on information that is not secret. Using secret parameters, however, message authentication cannot be forged unless the secret parameters are compromised. A different secret parameter is usually required for each sender-receiver pair. The logistics for distributing this secret information to the correct parties is analogous to key distribution for encryption (see below).

---

[15] S. Lipner, Digital Equipment Corp., personal communication with OTA staff, Dec. 24, 1986.

[16] Peter Schweitzer and Whitfield Diffie, personal communications with OTA staff, June 2, 1986.

[17] For a thorough discussion of message authentication and the various techniques used to authenticate messages, see Davies & Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfers*, Ch. 5, (New York, NY: J. Wiley, 1984). The descriptions of authentication techniques in this section follow Davies & Price closely.

[18] "Passive attack" is described as eavesdropping and "active attack" as the falsification of data and transactions through such means as: 1) alteration, deletion, or addition; 2) changing the apparent origin of the message; 3) changing the actual destination of the message; 4) altering the sequence of blocks of data or items in the message; 5) replaying previously transmitted or stored data to create a new false message; or 6) falsifying an acknowledgment for a genuine message. See Davies & Price, pp. 119-120.

If privacy as well as authentication is required, one scheme for encrypting and authenticating a message involves sequential use of DES with two different secret keys: one to calculate the authenticator (called the message authentication code or MAC) and one to encrypt the message. Even the use of a message authentication code and encryption do not safeguard against replay of messages or malice on the part of one of the corresponding parties, so various message sequence numbers, date and time stamps, and other features are usually incorporated into the text of the message. Box C discusses the use of message authentication in financial transactions. Figure 14 shows a data authentication code (synonymous with message authentication code) based on the DES algorithm.

Box C.—Application of Message Authentication to Electronic Funds Transfer

Developments in the banking industry provide a good example of how important information should be safeguarded, both because of the large amounts of money involved and because of the early use of new safeguard technology by segments of this industry.[1] Roughly $668 billion per day was transferred over the FedWire and Clearing House Interbank Payment System (CHIPS) networks alone in 1984, representing a 48 percent increase over 1980.[2] The fully-automated, online, FedWire system handled 49.5 million domestic transactions in 1986, with an average value of $2.5 million each, for a total of $124.4 trillion. In the same year, CHIPS handled $125 trillion in domestic and international payments for its member banks.[3]

During recent decades, the financial community has made increasing use of computer and communications systems to automate these fund transfers and other transactions. Typically, the computer systems of these financial institutions are interconnected with local and long distance public and private communications networks, over which the bankers have only limited control over potential fraud, theft, unauthorized monitoring, and other misuse. Their customers have an expectation of privacy and banks have the obligation to restrict details of financial transactions to those who need to know.

Wholesale and retail banking systems have somewhat different requirements for safeguards for funds transferred electronically. Wholesale bankers' requirements include message authentication and verification, as well as confidentiality of some communications; retail banking requirements additionally include authentication of individual automatic teller machines, confidentiality of customers' personal identification numbers, and communications security between the automatic tellers and the host computer. These needs are in sharp contrast with those of the defense-intelligence establishment, where confidentiality is the primary concern.

During the past decades, various technical methods have been adopted to reduce errors and to prevent criminal abuse relating to electronic fund transfers. Among these are parity checks, checksums, testwords, and pattern checks.[4] Some of these methods are widely used in various banking networks to verify that user inputs are correct and detect errors rather than protect against criminal activity.

---

[1] Wholesale banking transactions are characterized by large dollar amounts per average transaction (e.g., about $3 million) and daily volumes of transactions that number in the thousands or tens of thousands. Retail banking transactions amounts might average $50 and number in the hundreds of thousands.

[2] "Electronic Funds Transfer Systems Fraud," U.S. Department of Justice, Bureau of Justice Statistics, NCJ-100461, April 1986.

[3] Information on FedWire and CHIPs from F. Young, Division of Federal Reserve Bank Operations, personal communication with OTA staff, Feb. 12, 1987.

[4] For a brief description of testwords (or test keys) in banking transactions, see M. Blake Greenlee, "Requirements for Key Management Protocols in the Wholesale Financial Services Industry," *IEEE Communications Magazine*, vol. 23, No. 9, September 1985.

One of the major, traditional drawbacks of encryption systems is that of key distribution. Each pair of communicating locations generally requires a matched, unique set of keys or codes, which have to be delivered in some way—usually by a trusted courier—to these users each time the keys are changed. (An alternative is to use a prearranged code book, which can be compromised, as has been well publicized in recent spy trials.) The key distribution problem rapidly becomes onerous as the number of communicators increases.[5] The discovery of the public-key algorithm, noted earlier, may alleviate some of the key distribution problems—for example, to distribute the secret keys to large networks of users.

In the late 1970s, the financial community was quick to realize the potential of the new cryptographic-based message authentication codes as a replacement for testwords. These codes allow major improvements in safeguards against both errors and intentional abuse, and facilitate the potential of future transaction growth. Thus, this community has pioneered industrywide technical standards both in the United States and worldwide.

The message authentication code is a cryptographically derived check sum based on processing the electronic fund transfer message with the DES algorithm (called the Data Encryption Algorithm in the financial services community) and a secret key.[6] The sender calculates the code and appends it to the message. The receiver calculates a code independently based on the same message, algorithm, and secret key. Most new bank authentication systems in use or in planning utilize DES to calculate the codes. If the code calculated by the receiver is identical to that sent with the message, then there is a high level of assurance that the originator is authentic and that the content of the received message is identical to that transmitted by the sender, with no alterations of any kind. Also, some banks authenticate and encrypt their wholesale electronic fund transfers whenever practical and in countries where encryption is legally permissible.[7]

---

[5] The number of pairs of separate keys needed in a network of "n" communicators, each pair of which requires unique keys, is $n(n-1)/2$. Thus, a network of 5 communicators requires 10 separate pairs of keys, while a network of 100 communicators requires 4,950 pairs of keys. These numbers pale when considering that 10,000 banks send fund transfers worldwide, the largest of which have thousands of keying relationships.

[6] For a thorough discussion of the properties of message authentication techniques, see R.R. Jueneman, S.M. Matyas, and C.H. Meyer, "Message Authentication," *IEEE Communications Magazine*, vol. 23, No. 9, September 1985.

[7] C. Helsing, Bank of America, personal communication with OTA staff, December 1986.

Public-Key Ciphers

A symmetric cipher is an encryption method using one key, known to both the sender and receiver of a message, that is used both to encrypt and decrypt the message. Obviously, the strength of a symmetric cipher depends on both parties keeping the key secret from others. With DES, for example, the algorithm is known, so revealing the encryption key permits the message to be read by any third party.

An asymmetric cipher is an encryption scheme using a pair of keys, one to encrypt and a second to decrypt a message.[19] A special class of asymmetric ciphers are public-key ciphers, in which the encrypting key need not be kept secret to ensure a private communication.[20] Rather, Party A can publicly announce his or her encrypting key, PK_A, allowing anyone who wishes to communicate privately with him or her to use it to encrypt a message. Party A's decrypting key (SK_A) is kept secret, so that only A or someone else who has obtained

---

[19] See Davies & Price, ch. 8, for a more complete discussion of asymmetric and public-key ciphers. A discussion of the underlying principles of public-key ciphers, including examples of the RSA and knapsack algorithms, is given in Martin E. Hellman: "The Mathematics of Public-Key Cryptography," *Scientific American*, vol. 241, No. 2, August 1979, pp. 146-157. A pictorial example of the RSA public-key method can be found in *Understanding Computers/COMPUTER SECURITY* (Alexandria, VA: Time-Life Books, 1986), pp. 112-117.

[20] The public-key concept was first proposed by Whitfield Diffie and Martin Hellman in their pathbreaking paper, "New Directions in Cryptography," *IEEE Trans. Inform. Theory*, IT-22, 6, November 1976, pp. 644-654.

Figure 14.—Federal Standard for Authentication

The DAA Authentication Process

A cryptographic Data Authentication Algorithm (DAA) can protect against both accidental and intentional, but unauthorized, data modification.

A Data Authentication Code (DAC) is generated by applying the DAA to data as described in the following section. The DAC, which is a mathematical function of both the data and a cryptographic key, may then be stored or transmitted with the data. When the integrity of the data is to be verified, the DAC is generated on the current data and compared with the previously generated DAC. If the two values are equal, the integrity (i.e., authenticity) of the data is verified.

The DAA detects data modifications which occur between the initial generation of the DAC and the validation of the received DAC. It does not detect errors which occur before the DAC is originally generated.

Generation of the DAC

The Data Authentication Algorithm (DAA) makes use of the Data Encryption Standard (DES) cryptographic algorithm specified in FIPS PUB 46. The DES algorithm transforms (or encrypts) 64-bit input vectors to 64-bit output vectors using a cryptographic key. Let D be any 64-bit input vector and assume a key has been selected. The 64-bit vector, O, which is the output of the DES algorithm when DES is applied to D, using the enciphering operation, is represented as follows.

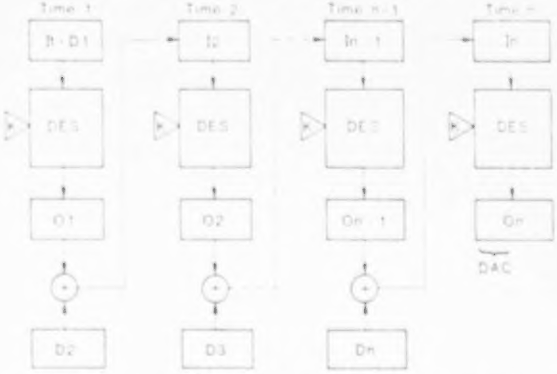
$O = e(D)$

The data (e.g., record, file, message, or program) to be authenticated is grouped into contiguous 64-bit blocks: D1, D2, . . ., Dn. If the number of data bits is not a multiple of 64, then the final input block will be a partial block of data, left justified, with zeros appended to form a full 64-bit block. The calculation of the DAC is given by the following equations where ⊕ represents the Exclusive-OR of two vectors.

$$O1 = e(D1)$$
$$O2 = e(D2 \oplus O1)$$
$$O3 = e(D3 \oplus O2)$$
$$\vdots$$
$$On = e(Dn \oplus On\text{-}1)$$

The DAC is selected from On. Devices which implement the DAA shall be capable of selected the leftmost M bits of On as the DAC, where $16 < M < 64$ and M is a multiple of 8. A block diagram of the DAC generation is given below, along with an example. The Cipher Block Chaining Mode (CBC) with Initialization Vector (IV) = O and the 64-bit Cipher Feedback Mode with IV = D1 and data equal to D2, D3, . . ., Dn (see FIPS PUB 81) both yield the required DAC calculation.

Block Diagram of the DAC Generation



D = Data Block
I = Input Block
O = Output Block
DES = Data Encryption Standard
K = DES Key
⊕ = Exclusive-OR

An Example of the DAA

Cryptographic Key = 0123456789abcdef

The text is the ASCII code for "7654321 Now is the time for." These 7-bit characters are written in hexadecimal notation $(0, b_7, b_6, \ldots, b_1)$.

Text =
37363534333231204e6f77206873207468652074696d652066f7220

TIME	PLAIN TEXT	DES INPUT BLOCK	DES OUTPUT BLOCK
1	3736353433323120	3736353433323120	21fb193693a16c28
2	4e6f772069732074	6f946e16fad24c5c	6c463f0cb7167a6f
3	68652074696d6520	04231f78de7b1f4f	956ee891e889d91e
4	666f722000000000	f3019ab1e889d91e	f1d30f6849312ca4

A 32-bit DAC = f1d30f68 is selected.

SOURCE: NBS FIPS Publication 113, May 30, 1985, pp. 3-6.

his or her decrypting key can easily convert messages encrypted with PK_A back into plaintext.[21] Knowing the public encrypting key, even when the encrypted message is also available, does not make computing the secret decrypting key easy, so that in practice only the authorized holder of the secret key can read the encrypted message.

If the encrypting key is publicly known, however, a properly encrypted message can come from any source. There is no guarantee of its authenticity. It is thus crucial that the public encrypting key be authentic. An imposter could publish his or her own public key, PK_I and pretend it came from A in order to read messages intended for A, which he or she could intercept and then read using his or her own SK_I. Therefore, the strength of the public-key cipher rests on the authenticity of the public key. A variant of the system allows a sender to authenticate messages by "signing" them using an encrypting key, which (supposedly) is known only to him or her. This very strong means of authentication is discussed further in the section on digital signatures below.

---

[21] For A and B to have private two-way communication, two pairs of keys are required: the "public" encryption keys PK_A and PK_B, and the secret decryption keys SK_A and SK_B.

The RSA public key is one patented system available for licensing from RSA Data Security, Inc. It permits the use of digital signatures to resolve disputes between a sender and receiver. The RSA system is based on the relative difficulty of finding two large prime numbers, given their product. The recipient of the message (and originator of the key pair) first randomly selects two large prime numbers, called *p* and *q*, which are kept secret. The recipient then chooses another (odd) integer *e*, which must pass a special mathematical test based on the values of *p* and *q*. The product, *n*, of *p* times *q* and the value of *e* are announced as the public encryption key. Even though their product is announced publicly, the prime factors *p* and *q* are not readily obtained from *n*. Therefore, revealing the product of *p* and *q* does not compromise the secret key, which is computed from the individual values of *p* and *q*.[22] Current implementations of the cipher use keys with 200 or more decimal digits in the published number N. A more complete description of the RSA system, including a discussion of its computational security, is given in appendix D.

Figure 15 shows a simple illustrative example of a public-key cipher based on the RSA algorithm. This simplified example is based on small prime numbers and decimal representations of the alphabet. It is important to bear in mind, however, that operational RSA systems use much larger primes.

The RSA system was invented at the Massachusetts Institute of Technology (MIT) in 1978 by Ronald Rivest, Adi Shamir, and Leonard Adelman. The three inventors formed RSA Data Security, Inc. in 1982 and obtained an exclusive license for their invention from MIT, which owns the patent. The firm has developed proprietary software packages implementing the RSA cipher on personal computer networks. These packages, being sold commercially, provide software-based communication safeguards, including message authentication, digital signatures, key management, and encryption. The firm also sells safeguards for data files and spread sheets transmitted between work stations, electronic mail networks, and locally stored files. The software will encrypt American Standard Code for Information Interchange (ASCII), binary, or other files on an IBM personal computers or compatible machines, and runs on an IBM PC/AT at an encryption rate of 3,500 bytes per second.

A number of public-key ciphers have been devised by other industry and academic researchers. Stanford University, for instance, holds four cryptographic patents, potentially covering a broad range of cryptographic and digital signature applications. Some of these patents have been licensed to various companies for use in their products.[23]

Digital Signatures

Encryption or message authentication alone can only safeguard a communication or transaction against the actions of third parties. They cannot fully protect one of the communicating parties from fraudulent actions by the other, such as forgery or repudiation of a message or transaction. Nor can they resolve contractual disputes between the two parties. Paper-based systems have long depended on letters of introduction for identification of the parties, signatures for authenticating a letter or contract, and sealed envelopes for privacy. The contractual value of paper documents hinges on the recognized legal validity of the signature and the laws against forgery.

---

[22] Certain special values of (p)(q) can be factored easily—when p and q are nearly equal, for instance. These special cases need to be avoided in selecting suitable keys. Furthermore, it is important to remember that this cipher system is no more secure than the secrecy of the private key.

[23] The companies include the Harris Corp., Northern Telecom, VISA, Public Key Systems, and Cylink. Lisa Kuuttila, Stanford Office of Technology Licensing, personal communication with OTA staff, Sept. 29, 1986.

Figure 15.—Public-Key Ciphers

This example is adapted from one used in *Understanding Computers/Computer Security*, © 1986 Time-Life Books, Inc.

A. Converting a message to numbers

Prescribed numeric values

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	•	,	.
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

Converting the message

S	E	L	L	•	1	0	0	•	S	H	A	R	E	S	•	O	F	•	A	B	C	D	•	I	N	D	U	S	T	R	I	E	S		•	J	O	H	N	•	S	M	I	T	H	
19	5	12	12	37	28	27	27	37	19	8	1	18	5	19	37	15	6	37	1	2	3	4	37	9	14	4	21	19	20	18	9	5	19	39	37	10	15	8	14	37	19	13	9	20	8	39

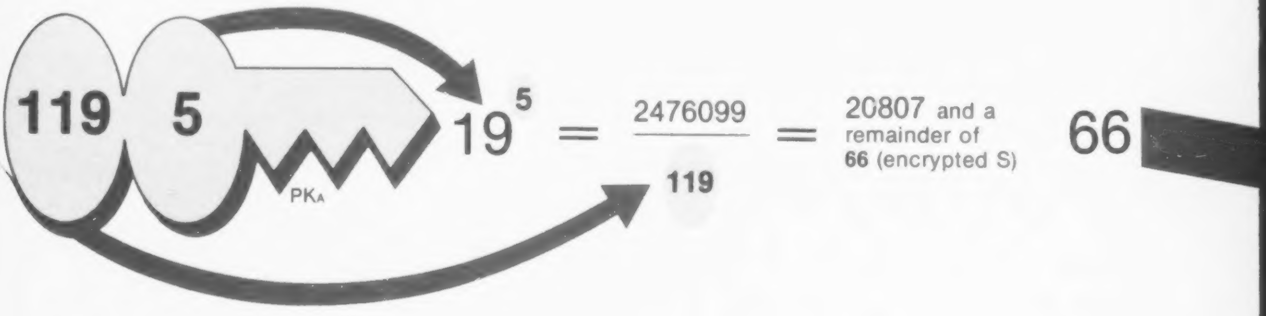
Before a message can be encrypted by the public-key method, it must be blocked and each block assigned a numerical value. Blocks may vary in size, from one character to several; and numerical values may be assigned in many ways, within constraints imposed by the system. In the example used here, each character is treated as a block, and a simple number-assigning system is used: A = 1, B = 2, C = 3, D = 4, and so on *(table at top)*.

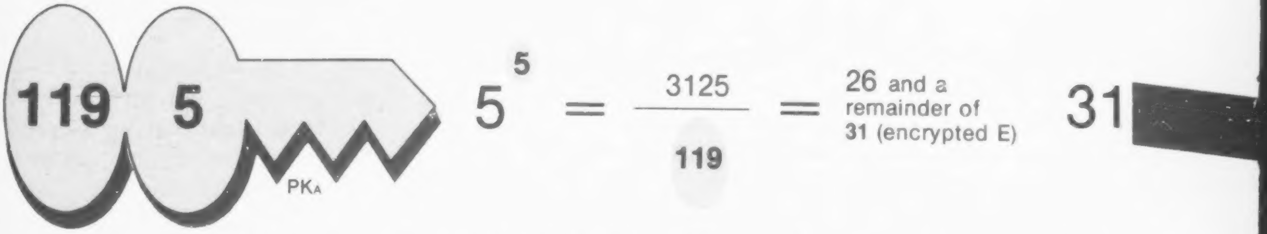
C. The Arithmetic of locking and unlocking: the sender, user B, uses PKA to encrypt a message to user A.

The number 19, assigned to the letter S, is raised to the fifth power (multiplied by itself five times), as dictated by the second part of PKA (5).

The result of 19 raised to the fifth power—2,476,099—is divided by the first part of PKA, the number 119.

The division yields the number 20,807 and a remainder of 66. Only the remainder is important. It is the value of the encrypted letter S.


119
5
PKA
$19^5 = \frac{2476099}{119} =$
20807 and a remainder of 66 (encrypted S)
66


119
5
PKA
$5^5 = \frac{3125}{119} =$
26 and a remainder of 31 (encrypted E)
31

The next letter of the message, E, has the assigned value 5. Using the second part of PKA, this number is raised to the fifth power.

The result of multiplying 5 by itself five times—3,125—is divided by the other part of PKA 119.

The division yields the number 26 and a remainder of 31. Again, only the remainder is significant. it is the value of the encrypted letter E.

B. Creating user A's keys.

1. Each user has a public and a private key, and each key has two parts. To create user A's keys, two prime numbers, customarily designated P and Q, are generated by an operator at a central computer or key generation center. (To qualify, a prime number must pass a special mathematical test.) Here, P is 7, Q is 17.

2. In this simplified example, the two primes are multiplied, and the result—N—will be the first part of both keys, N is 119.

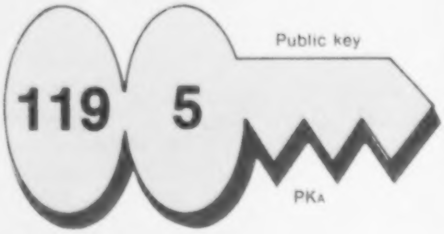
3. Next, an odd number is chosen, in this case, 5. (This number—designated E—must also pass a special mathematical text.) It forms the second part of the public key, PKA.

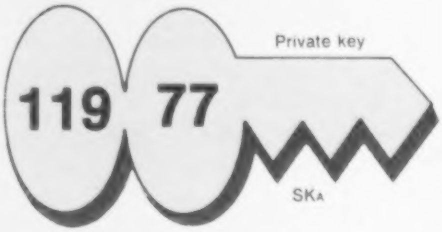
4. To create the second part of the private key, the numbers are multiplied: P minus 1 (6, in this case) times Q minus 1 (16) times E minus 1 (4). The result is 384.

5. Next, 1 is added to the result of the previous step, yielding 385.

6. The sum is divided by E (5). The result of the division, 77 (designated D), is the second part of SKA.

1 P = 7, Q = 17
2 $7 \times 17 = 119 =$ N
3 E = 5
4 $6 \times 16 \times 4 =$ 384
5 $384 + 1 = 385$
6 $385 \div 5 = 77 =$ D





At the end of the procedure user A has a public key (119 5) and a private key (119 77). In reality, these numbers would be many digits long.

D. The recipient, user A, uses his private key, SKA, to decrypt the message.

Decryption, using SKA, follows the same steps. First, 66—the encrypted S—is raised to the 77th power, as dictated by the second part of the key, SKA.

The result of the previous step is divided by 119, the first part of SKA, which is identical to the first part of user A's public key.

The remainder resulting from the division is 19—the original number assigned to the letter S. Thus, the decryption of the first one-letter block of the message is complete.

$66^{77} = \frac{1237\ldots}{119} =$ 1069 . . . and a remainder of **19** (numerical equivalent of) S

$31^{77} = \frac{6836\ldots}{119} =$ 5745 . . . and a remainder of **5** (numerical equivalent of) E

The number 31—the encrypted letter E—is raised to the 77th power, as dictated by the second part SKA.

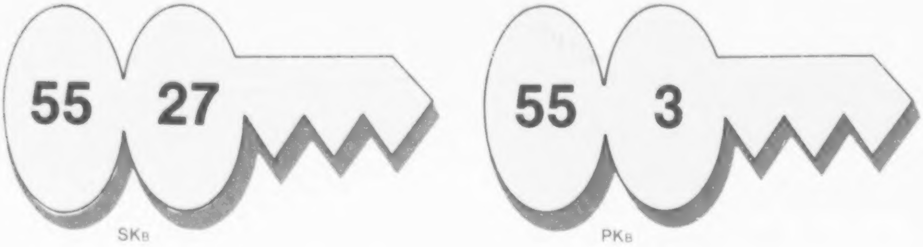
The result of multiplying 31 by itself 77 times is divided by 119, the other part of the private key SKA.

The remainder from the division is 5—the original value assigned to the letter E. Each letter block will be decrypted in the same way.

SOURCE: Adapted from *Computer Security* (Alexandria, VA: Time-Life Books, 1986), pp. 112-115.

Figure 16.—Digital Signatures Using a Public-Key Cipher

This example uses the same key pair (PK_A, SK_A) generated for user A in figure 15. In this example, the sender (user B) uses his private key (SK_B) to "sign" a message intended for user A and then "seals" it by encrypting, the message with user A's public key (PK_A).



User B's private key

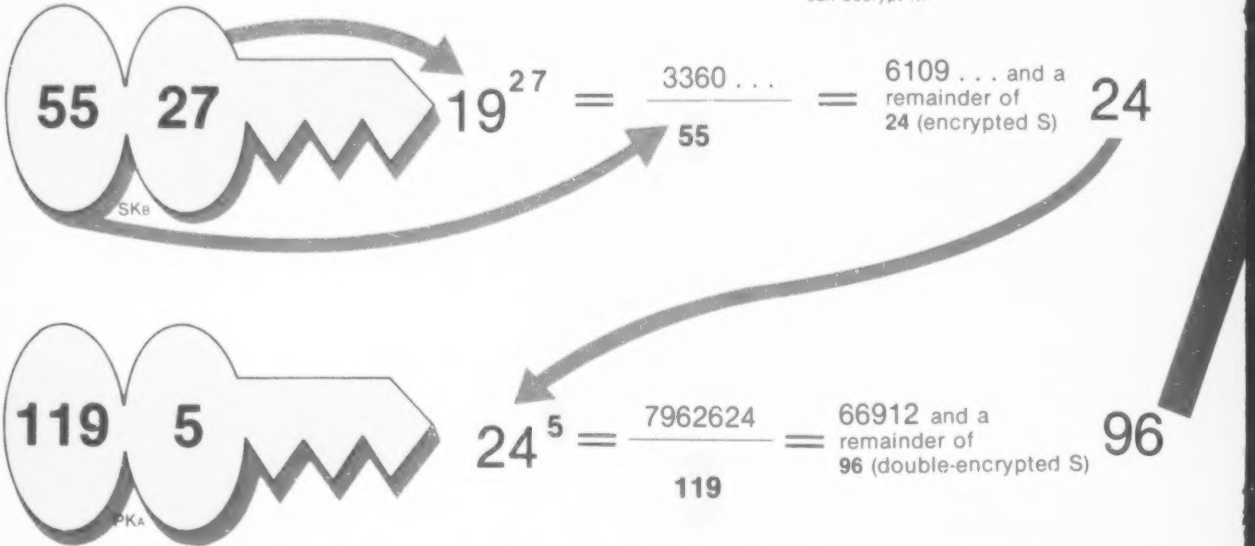
User B's public key

When user A receives the signed and sealed message, he uses his SK_A to unseal the message and the sender's PK_B to unsign it.

To begin the encryption technique called signing, the value of the letter S (19)—is raised to the 27th power, as dictated by the second part of SK_B.

The result of raising 19 to the 27th power is divided by 55, the first part of SK_B.

The division yields a very large number, which is disregarded, and a remainder of 24. This completes the signing process for the letter S; only user B's public key PK_B can decrypt it.


55
27
SK_B
$19^{27} = \frac{3360\ldots}{55} =$
6109 . . . and a remainder of **24** (encrypted S)
24
119
5
PK_A
$24^5 = \frac{7962624}{119} =$
66912 and a remainder of **96** (double-encrypted S)
96

To seal the message for secrecy, the result of the first encryption, 24 in this case, is raised to the fifth power, as dictated by the second part of the receiver's public key, PK_A.

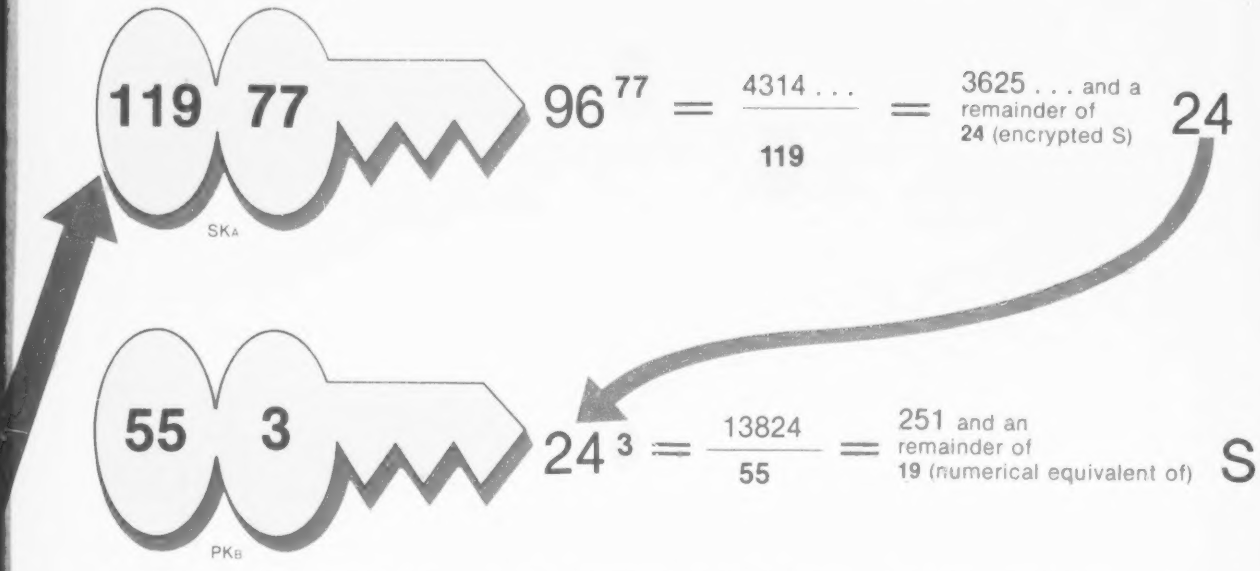
The result of raising 24 to the fifth power is divided by 119, the other part of PK_A.

The division yields a number (disregarded) and a remainder of 96—the twice-encrypted S. It will be sent when the rest of the message has undergone the same double encryption.

To decrypt a signed-and-sealed message, user A raises the number 96—the double-encrypted S—to the 77th power, as dictated by one part of his private key, SKA.

The result of the previous step is divided by 119, the other part of SKA.

The division yields a very large number (disregarded) and a remainder of 24—the cipher imposed on the letter S by the sender's private key, SKB.


119
77
SKA
96 77 = 4314 . . . / 119 = 3625 . . . and a remainder of 24 (encrypted S)
24
55
3
PKB
24 3 = 13824 / 55 = 251 and an remainder of 19 (numerical equivalent of)
S

To decrypt this digital signature, the number 24 is raised to the third power, as dictated by one part of the sender's public key, PKB.

The result of raising 24 to the third power is divided by 55, as determined by the other part of PKa.

The division yields a number (disregarded) and a remainder of 19—the numerical equivalent assigned to the letter S by the system. Performing the same steps on the rest of the transmission reveals the plaintext.

SOURCE: Adapted from *Computer Security* (Alexandria, VA: Time-Life Books, 1986), pp. 116-117.

Equivalent functions for electronic documents can be provided by using an asymmetric cipher, such as the RSA cipher, to create a digital signature for a document.[24] This can both authenticate their contents and also prove who sent them because only one party is presumed to know the secret information used to create the signature. If privacy is required, encryption can be used in addition to the digital signature. However, the "proof" of the signature hinges on the presumption that only one party knows the secret signing key. If this secret information is compromised, then the proof fails.

The equivalent of a letter of introduction is still necessary to verify that the correct public key was used to check the digital signature—an adversary might try to spoof the signature system by substituting his or her own public key and signature for the real author's. This letter of introduction could be accomplished by several means. The system offered by RSA Data Security, Inc., provides "signed key server certificates" by attaching the corporation's own digital signature to its customers' public keys. Thus, customers can attach their certified public keys to the messages they sign. Note that although a public-key cipher system is used to set up the digital signature system, the actual text of the message can be sent in plaintext, if desired, or it can be encrypted using DES or the public-key cipher.[25]

Figure 16 continues the simplified example in figure 15 to illustrate the digital signature technique.

---

[24] Other public-key ciphers using different one-way functions could provide the mechanism for a form of digital signature; however, none are commercially available at present. Also, it is possible to use a symmetric cipher such as DES in an asymmetric fashion—at least two signature functions of this type have been described—but these functions are more inconvenient to use than the RSA method and require more administrative effort. See Davies & Price, ch. 9, for a general treatment of digital signatures and alternative methods.

[25] For example, if the author wishes to keep the text of the message private, so that only the intended recipient can read it, he or she can encrypt the signed message, using the recipient's public key. Then, the recipient first uses his or her own secret key to decrypt the signed message and then uses the sender's public key to check the signature. In practice, the RSA digital signature system is used to transmit a DES key for use in encrypting the text of a message because DES can be implemented in hardware and is much faster than using the RSA algorithm to encrypt text in software.

NEW TECHNOLOGIES FOR PRIVATE AND SECURE TRANSACTIONS

The public-key and digital signature systems described above have important uses for key exchange and management, for authenticating messages and transactions, and for permitting enforceable "electronic contracts" to be made, including electronic purchase orders and other routine business transactions. Digital signatures might also be used in equally secure transaction systems that preserve the privacy of individuals. This would be accomplished by permitting transactions to be made pseudonymously (using digital signatures, which would correspond to digital pseudonyms that could differ for each type of transaction).[26] That is, transactions could be made without revealing the identity of the individual, yet at the same time making certain that each transaction is completed accurately and properly.

---

[26] See, for example, David Chaum, "Security Without Identification: Transactions Systems To Make Big Brother Obsolete," *Communications of the ACM*, vol. 28, No. 10, October 1985.

Digital signatures could prevent authorities from cross-matching data from different types of transactions or using computer profiling to identify individuals who have a particular pattern of transactions. Database matching is a technique that uses a computer to compare two or more databases to identify individuals in common (e.g., Federal employees who have defaulted on student loans). Computer profiling uses inductive logic to determine indicators of characteristics and/or behavior patterns that are related to the occurrence of certain behavior (e.g., developing a set of personal and transactional criteria that make up a profile of a drug courier).[27]

Public-key systems make it possible to establish a new type of transaction system that protects individual privacy while maintaining the security of transactions made by individuals and organizations. This new system would create a security relationship between individuals and organizations in which an organization and the individuals it serves cooperatively provide mutual protection, allowing the parties to protect their own interests.

For example, instead of individuals using the same identification (e.g., Social Security numbers, which are now commonly used on drivers' licenses, insurance forms, employment records, tax and banking records, etc.), they would use a different account number or digital pseudonym with each organization they do business with. Individuals could create their pseudonyms, rather than have them issued by a central authority. A one-time pseudonym might even be created for certain types of transactions, such as retail purchases. Although individuals would be able to authenticate ownership of their pseudonyms and would be accountable for their use, the pseudonyms could not be traced by computer database matching.[28] On the other hand, the use of numerous digital pseudonyms might make it more complicated for individuals to check or review all their records.[29]

A second difference is the ownership of the "tokens" used to make transactions. Currently, individuals are issued credentials, such as paper documents or magnetic stripe cards, to use in transactions with organizations. Moreover, the information contained on the electronic credentials is usually not directly reviewable or modifiable by the individual who uses it. In the scheme described above, individuals would own the transaction token and would control the information on it.

This system illustrates how technological developments and organizational changes can be used to mitigate potential erosions of privacy that could result from the widespread use of multi-purpose smart cards and computer profiling. However, while the technology and organizational infrastructures for the latter, at least, are already fairly well developed, the practical development of privacy systems is just beginning.[30]

KEY MANAGEMENT

Key management is fundamental and crucial to encryption-based communication and information safeguards. As an analogy, one might say that:

> The safety of valuables in a locked box depends as much or more on the care with which the keys are treated than on the quality of the lock. It is useless to lock up valuables if the

---

[27] For a further discussion of the implications of computer database matching and profiling, see the Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986).

[28] A formal description of a "credential mechanism" for pseudonyms is given in David Chaum and Jan-Hendrik Evertse, "A Secure and Privacy-Protecting Protocol for Transmitting Personal Information Between Organizations," *Advances in Cryptology: Proceedings of Crypto 86*, A.M. Odlyzko (ed.), Springer-Verlag Lecture Notes in Computer Science, forthcoming, summer 1987.

[29] Chaum suggests using a card computer to manage this complexity while maintaining a convenient user interface. Personal communication with OTA staff, February 1987.

[30] The Center for Mathematics and Computer Science in Amsterdam has recently demonstrated a payment system and is working with European groups to develop trial systems. David Chaum, personal communication with OTA staff, February 1987.

> key is left lying around. The key may be stolen, or worse, it may be secretly duplicated and used at the thief's pleasure.[31]

Key management encompasses the generation of encrypting and decrypting keys as well as their storage, distribution, cataloging, and eventual destruction. These functions may be handled centrally, distributed among users, or by some combination of central and local key management. Also, key distribution can be handled through various techniques: by using couriers to distribute data-encrypting keys or master (key-encrypting) keys, for instance, or by distributing keys electronically using a public-key cipher. The relative merits of each mode of key management are subject to some debate.

For example, some technical experts, including those at NSA, argue that centralized key generation and distribution, perhaps performed electronically, efficiently ensures interoperability among different users and that relatively unsophisticated users do not inadvertently use any weak keys that may exist. NSA has stated that, for reasons of security and interoperability, it plans to control key generation for the new STU-III secure telephones (see ch. 5), including those purchased by private sector users. It is also likely that NSA will control key generation for equipment using its new encryption modules.

Some critics of this plan are concerned that NSA might be required—by secret court order, perhaps—to selectively retain certain users' keys in order to monitor their communications. Others express concerns that keying material may be exposed to potentially unreliable employees of NSA contractors. At the very least, the prospect of centralized NSA key generation has generated some public controversy.

On the other hand, the National Bureau of Standards (NBS) operates on the assumption that each user organization should generate its own keys and manage its own key distribution center. In the United States, Federal standards for protecting unclassified information in Government computer systems have been developed by NBS[32] which has also worked cooperatively with private organizations such as the American Bankers Association (ABA) and the American National Standards Institute (ANSI). Additionally, ABA and ANSI have developed voluntary standards related to cryptography for data privacy and integrity, including key management. The International Organization for Standardization (ISO) has been developing international standards, often based on those of NBS and/or ANSI.[33] Standards of these types are intended to specify performance requirements (accountability for keys, assignment of liability) and interoperability requirements for communications among users.

According to some experts, it is technically possible to handle centralized key distribution so that the key-generating center cannot read users' messages. If this were done, it would provide efficient and authenticated key distribution without the potential for misuse by a centralized authority. However, whether NSA plans to use these techniques has not been made public.

In any event, a key distribution center of some sort is the most prominent feature of key management for multi-user applications. Such a center is needed to establish users' identities and supply them with the keys to be used for communications—usually, with "seed" keys used to establish individual session keys.

---

[31] This analogy is from Lee Neuwirth: "A Comparison of Four Key Distribution Methods," *Telecommunications* (Technical Note), July 1986, pp. 110-115. For a detailed discussion of key distribution and key management schemes, also see ch. 6 of Davies & Price.

[32] See, for example, Federal Information Processing Standards (FIPS) Publications FIPS PUB 81, 74, and 113 published by NBS.

[33] D. Branstad, Institute for Computer Science and Technology, National Bureau of Standards. Information about NBS and standards development from personal communication with OTA staff, Aug. 6, 1986. For a general discussion of security standards based on cryptography, see: Dennis K. Branstad and Miles E. Smid, "Integrity and Security Standards Based on Cryptography," *Computers and Security*, vol. 1, 1982, pp. 255-260.

Even in a public-key system, the initial secret keys must be computed or distributed. NBS has developed a key notarization system that provides for authenticated distributed keys and other key management functions.[34] NBS had initiated a process for developing standards for public-key systems[35] but is no longer pursuing this activity.

The traditional means of key distribution—through couriers—is a time-consuming and expensive process that places the integrity of the keys, hence the security of the cipher system, in the hands of the courier(s). Courier-based key distribution is especially awkward when keys need to be changed frequently. Recently, public-key systems for key distribution have been made available allowing encryption keys (e.g., DES keys) to be securely transmitted over public networks—between personal computers over the public-switched telephone network, for example. There continue to be new developments in public-key cryptography research.[36]

To date, the best-known commercial offering of a public-key system to secure key distribution (or other electronic mail or data transfers) is by RSA Data Security, Inc. Other public-key systems have been developed, some earlier than RSA, but to date none have yet gained wide commercial acceptance. Although RSA initially attempted to implement its algorithm in hardware, their first successful commercial offerings, introduced in 1986, use software encryption. The Lotus Development Corp., one of the largest independent software companies, has licensed the RSA patent for use in future products. RSA Data Security has also licensed the patent to numerous large and small firms and to universities engaged in research, as well as to some Federal agencies, including the U.S. Navy and the Department of Labor.[37] A new hardware implementation of several public-key ciphers (including RSA and the SEEK cipher) was offered commercially in 1986. The chip, developed by Cylink, Inc., will be used in Cylink's own data encryption products and is available to other vendors who wish to use it.[38]

VOICE AND DATA COMMUNICATIONS ENCRYPTION DEVICES

A number of commercial products, in the form of hardware devices or software packages, are available to encrypt voice and data communications. Software-based encryption is slower than hardware encryption and many security experts consider it to be relatively insecure (because, among other reasons, the encryption keys may be "exposed" in the computer operations). Still, some commercial users prefer software encryption because it is relatively inexpensive, does not require additional hardware to be integrated into their operations, and is compatible with their existing equipment and operations. However, this section will deal only with hardware products, in large part because only hardware products have been certified for Government use.

Since 1977, NBS has validated 28 different hardware implementations of the DES algorithm (in semiconductor chips or firmware), but NBS does not validate vendors' software implementations of the algorithm. In 1982, the General Services Administration (GSA) issued Federal Standard 1027, "Telecommunications: Interoperability and Security Requirements for Use of the DES, in the Physical Layer of Data Communications." At present, equipment purchased by Federal agencies to protect unclassified information must meet FS 1027 specifications; vendors may submit products built using validated DES chips or firmware to NSA for FS 1027 certification. NSA has a DES endorsement program to certify products for government use, but plans to dis-continue this program on January 1, 1988. As stated earlier in this chapter, DES products endorsed prior to this date can be used indefinitely.[39]

---

[34] Branstad and Smid, op. cit., p. 258.

[35] Ibid., p. 259.

[36] S. Goldwasser, S. Micali, and R. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen Message Attack," MIT Laboratory for Computer Science, Rev. Apr. 23, 1986.

[37] Letter to OTA staff from Jim Bidzos, RSA Data Security, Inc., Feb. 19, 1987.

[38] See "Cypher Chip Makes Key Distribution A Snap," *Electronics*, Aug. 7, 1986, pp. 30-31.

Hardware encryption products use special semiconductor or firmware devices to implement one or more encryption algorithms. Online encryption (in which data is encrypted as it is transmitted and decrypted as it is received, as opposed to off-line encryption in which plaintext is first encrypted and then stored for later transmission) can be implemented in two ways. In the first method, called end-to-end encryption, synchronized encryption/decryption devices at the source and destination operate so that the transmitted information is encrypted and remains in its encrypted form throughout the entire communications path. In the second method, called link encryption, the transmitted information is also encrypted at the source, and decrypted and then reencrypted at each intermediate communications node between the source and the ultimate destination. Thus, the information is encrypted, decrypted, and reencrypted as it traverses each link along its communications path.

By late 1986, the market research firm DataPro listed about 30 vendors that were marketing commercial encryption equipment, using the DES and/or proprietary algorithms, and operating at low or high data rates (depending on the product and vendor, encryption data rates can range from about 100 bits per second up to 7 million bits per second). These vendors offer 40 or more commercial products or families of products, mostly for data encryption, although a few vendors offer products for voice encryption. Some vendors specialize in encryption-only products, while others are data communications service (turnkey) providers offering encryption products complementing the rest of their product line. Published prices range from $500 to several thousand dollars per unit, depending on data rate and other features.

PERSONAL IDENTIFICATION AND USER VERIFICATION

Background

User verification measures aim to ensure that those who gain access to a computer or network are authorized to use that computer or network. Personal identification techniques are used to strengthen user verification by increasing the assurance the person is actually the authorized user.[40]

User verification techniques typically employ a combination of (usually two) criteria, such as something an individual has, knows, or is. Until recently, the "has" has tended to be a coded card or token, which could be lost, stolen, or given away and used by an unauthorized individual; the "knows" a memorized password or personal identification number, which could be forgotten, stolen, or divulged to another; and the "is" a photo badge or signature, which could be forged. Cards and tokens also face the problem of counterfeiting.

Now, new technologies and microelectronics, which are harder to counterfeit, are emerging to overcome the shortcomings of the earlier user verification methods. At the same time, these new techniques are merging the has, knows, or is criteria, so that one, two, or all three of these can be used as the situation dictates. Microelectronics can make the new user verification methods compact and portable. Electronic smart cards, for example, now carry prerecorded, usually encrypted, access control information that must be compared with data that the proper authorized user is required to provide, such as a memorized personal identification number or biometric data like a fingerprint or retinal scan.

---

[39] Harold E. Daniels, Jr., Deputy Director for Information Security, NSA, enclosure 3, page 4 in letter S-0033-87 to OTA, Feb. 12, 1987.

[40] Purists will note that the "personal identification" systems in common use do not actually identify a person, rather they recognize a user based on pre-enrolled characteristics. The term "identification" is commonly used in the industry, however.

Merging the criteria serves to authenticate the individual to his or her card or token and only then to the protected computer or network. This can increase security since, for example, one's biometric characteristics cannot easily be given away, lost, or stolen. Moreover, biometrics permit automation of the personal identification/user verification process.

While false acceptances and false rejections can occur with any identification method, each technique has its own range of capabilities and attributes: accuracy, reliability, throughput rate, user acceptance, and cost. As with other security technologies, selecting an appropriate system often involves trade-offs. For one thing, elaborate, very accurate technical safeguards are ineffective if users resist them or if they impede business functions. The cost and perceived intrusiveness of a retina scanner might be acceptable in a high-security defense facility, for example, but a relatively low-security site like a college cafeteria might sacrifice high reliability for the lower cost, higher throughput rate, and higher user acceptance of a hand geometry reader. In banking, where user acceptance is extremely important, signature dynamics might be the technology of choice. In retail sales, a high throughput rate is extremely important and slower devices would not be acceptable.

Access control technologies will evolve for niche markets. Successful commercial products for the defense and civilian niches will look very different. As of early 1987, there were no specific performance standards for most of these user verification technologies, but it is likely that these will be developed. One incentive for the development of access control standards, at least for the Government market, is the access control objectives specified in the so-called "Orange Book."[41] The development of user verification technologies, however, is being driven significantly by commercial needs. In the area of biometrics, vendors have formed an industry association. The International Biometrics Association is beginning to address industry issues including performance and interface standards and testing and has a standing committee on standards and technical support.

In short, the new access control technologies are moving toward the ideal of absolute personal accountability for users by irrefutably tying access and transactions to a particular individual. Some enthusiasts and industry experts foresee great and pervasive applications for some of the access control technologies, even to their evolution into nonsecurity applications, such as multiple-application smart cards (see above). However, a given set of access control technologies cannot, in themselves, fix security problems "once and for all." Changes in information and communication system infrastructures can eventually undermine previously effective safeguards. Therefore, safeguards have a life cycle. It is the combination of attributes, of the safeguard technique, and of the system it seeks to protect that determines the useful life of a safeguard.

Conventional Access Controls

Password-Based Access Controls

The earliest and most common forms of user verification are the password or password-based access controls. The problem is that passwords can be stolen, compromised, or intentionally disclosed to unauthorized parties. In addition, trivial passwords can easily be guessed and even nontrivial ones can be broken by repeated attack.[42] Once stolen or compromised, passwords can be disclosed widely or even posted on electronic bulletin boards, resulting in broad exposure of a system to unauthorized access. If operating system security is poor, one user who unilaterally compromises his or her own password can compromise the whole system. An even more serious weakness is that, because there may be no tangible evidence of a security breach, a compromised password can be misused over and over until either the password is routinely changed, its compromise is discovered, or other events occur (e.g., data are lost or fraudulently changed). To avoid some of these problems, many modern systems use special procedures to frustrate repeated incorrect attempts to log on.

---

[41] Department of Defense Trusted Computer System Evaluation Criteria. Department of Defense Standard DOD 5200.28-STD, December 1985. Section 7.4 of the Orange Book specifies that individual accountability must be ensured whenever classified or sensitive information is processed. This objective encompasses the use of user verification, access control software, and audit trails.

[42] Common password misuses include sharing one's password with other users (including friends or co-workers), writing down the "secret" series of letters or numbers for reference and storing it in an unsecure place (examples of this abound, including writing passwords or identification numbers on the terminals themselves or on desk blotters, calendars, etc., or storing them in wallets or desk drawers), and permitting others to see the log-on/authorization code being keyed in at the terminal. Some password schemes allow users to select their own passwords; while this increases the secrecy of the passwords because they are known only by the users, trivial password choices can reduce security if the passwords are easy to guess (examples of trivial passwords would be a pet's name, a birthdate, or license plate number).

Until the last decade or so all access points to computer systems could be physically identified, which simplified the system administrator's job of controlling access from them. In addition, users could be easily defined and their terminals had limited capabilities. A network of this type is shown in figure 17.

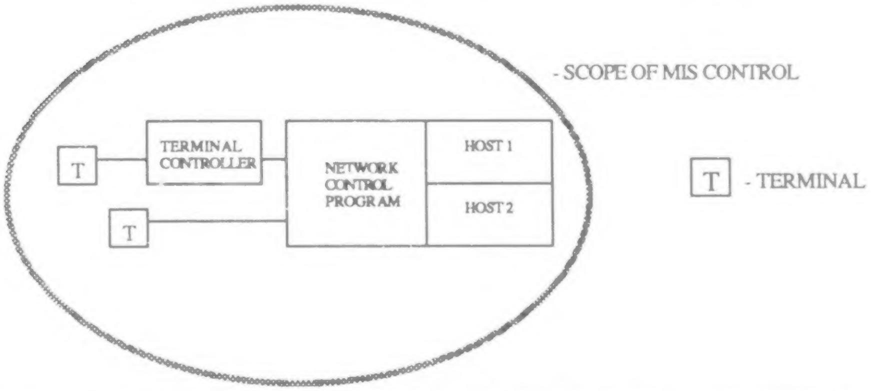
Now, new network configurations have emerged, characterized by personal computers linked to local area networks and connected by fixed and/or public switched telephone lines, as shown in figure 18. Users can readily extend the network by connecting modems to personal computers for pass-through access.

As a result, it is no longer possible to identify all access points. Communication nodes are no longer controlled exclusively by the organization when, for example, authorized users need to gain access from remote locations. While pass-through techniques facilitate access by authorized users, they can also be misused. For example, under some circumstances they can be used to defeat even such security techniques as call-back modems. With the increased number of network access points, the intrinsic weaknesses of the password further exacerbate the system's vulnerabilities.

Token-Based Access Controls

Network evolution, therefore, has made user identification and authentication even more critical. Some of the new access-control technologies can see through the communications network to the end user to authenticate him or her—at least as the "holder" of the proper

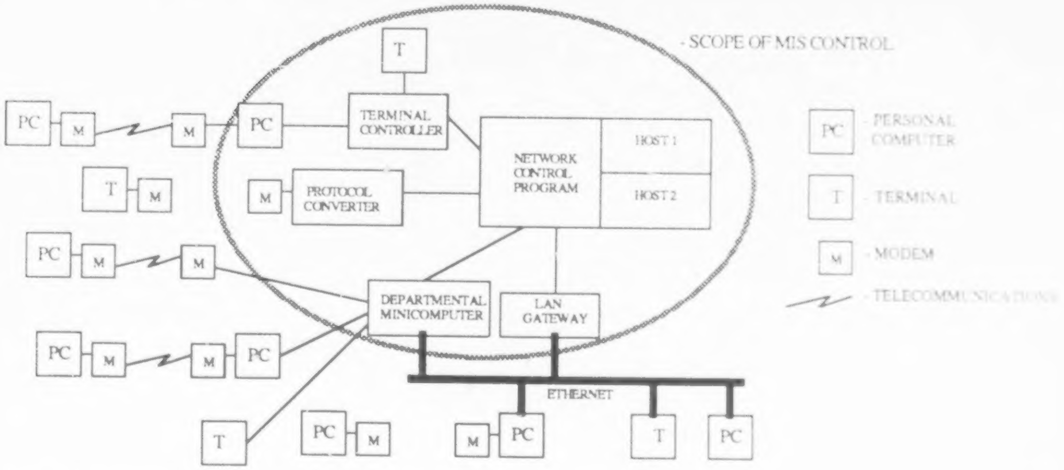
Figure 17.—A Description of the Past Network Environment



In the past network environment, control of all network resources resided with systems professionals. Typically, fixed-function terminals were direct-connected to the mainframe or a terminal controller. The communications parameters were specified through tables in the network control program (NCP), also under the direction of the systems group. As a result, the network was totally under the custodianship of systems professionals.

SOURCE: Ernst & Whinney, prepared under contract to OTA, November 1986.

Figure 18.—A Description of the Current/Future Network Environment



In the current/future network environment, systems professionals still control direct connection to the mainframe. Through the network control program (NCP), they maintain the communications parameters that control the access through the devices directly connected to the mainframe. However, the nature of these devices is changing dramatically. Instead of fixed-function terminals, they now consist of departmental minicomputers, local area network (LAN) gateways, and personal computers. All of these devices have the capability to expand the network beyond the scope of mainframe control. This environment invalidates many of the premises upon which conventional access control mechanisms, such as passwords and call-back modems, were based.

SOURCE: Ernst & Whinney, prepared under contract to OTA, November 1986.

token—regardless of his or her physical location. Within the limitations of current technology, token-based systems are best used in combination with a memorized password or personal identification number identifying the user to the token.

In contrast to the password, token-based systems offer significantly greater resistance to a number of threats against the password system. Many token-based systems are commercially available. By December 1986, two of these had been evaluated by NSA's National Computer Security Center (NCSC) and approved for use with the access control software packages on NCSC's Evaluated Products List. (See ch. 5 for a discussion of NSA's programs.)

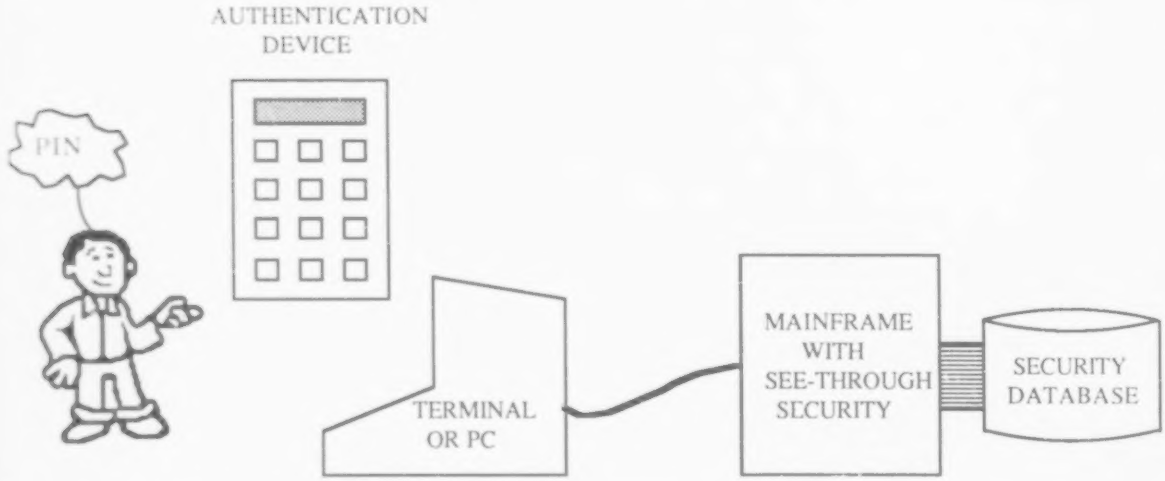
Token-based systems do much to eliminate the threat of external hackers. Under the token-based system, the password has become a one-time numeric response to a random challenge. The individual's memorized personal identification number or password to the token itself may be trivial, but the external hacker will ordinarily not have physical access to the device, which is usually designed to be tamper-resistant and difficult to counterfeit.

Hackers also have been known to make repeated tries at guessing passwords, or make use of overseen, stolen, or borrowed passwords. Repeated attack of the password to the host is also thwarted because this password is a random number and/or an encryption-based, one-time response from the token. The one-time nature of the host password also eliminates its compromise through observation, open display, or any form of electronic monitoring. As soon as a response is used, it becomes invalid. A subsequent access request will result in a different challenge from the host and a different required response from the token. An individual user can still unilaterally compromise the authentication process by giving away his or her token and memorized identification number. However, in this case, that individual no longer has access. In this way, the loss of a token serves as a warning that authentication may be compromised.

The see-through token (figure 19), used with a password, is an active device requiring complementary user action. Systems of this type currently on the market do not physically connect to a terminal, but instead provide a one-time user password for each access session. Tamper-proof electronics safeguard against reverse engineering or lost or stolen tokens. Some versions of these devices can challenge the host, effectively countering attempts at spoofing.

Two types of see-through tokens are currently available from several vendors: auto-

Figure 19.—The Mechanics of See-Through Security



Typical flow of events in a see-through security authentication session
1. User requests access to host through terminal or PC; enters user ID.
2. Host calculates random number (challenge) and transmits it to terminal.
3. User identifies himself to authentication device by entering Personal Identification Number (PIN), or through biometric identification.
4. User enters challenge from host into authentication device. Device uses the security algorithm and the user seed (both in device memory and inaccessible to the user) to calculate a numeric response.
5. User sends numeric response to host via the terminal.
6. Host calculates a response using the same challenge number, the security algorithm, and the user's seed from the security database. Host compares its response to user response, and grants or denies access.

SOURCE: Ernst & Whinney, prepared under contract to OTA, November 1986.

matic password generators, synchronized with the host, and challenge/response devices, using numerical key pads or optical character readers. According to some security consultants, these see-through techniques will be commonplace by the 1990s.[43]

Incorporating biometrics into these techniques will produce powerful safeguards, but there are associated risks. If biometric templates or data streams containing biometric information are compromised, the implications can be quite serious for the affected individuals because the particular measurements become invalid as identifiers. These risks can be minimized by properly designing the system so that biometric data are not stored in a central file or transmitted during the user verification procedure (as they would be in a host-based lookup mode). For many, therefore, the preferred operation for biometrics would be in a stand-alone mode, with the user carrying a biometric template in a token (like a smart card). However, tokens can be lost or stolen, and placing the biometric template on the token removes it from direct control by system security personnel. For these reasons, some installations, especially very high-security facilities using secure computer operating systems, may prefer host-based modes of operation. Figure 20 illustrates the differences between host-based and stand-alone modes for biometrics.

Biometric and Behavioral Identification Systems

There are three major classes of biometric-based identification systems that are commercially available for user verification and access control. Since each of these systems is based on a different biometric principle, they vary widely in their technologies, operation, accuracy, and potential range of applications. The three classes are based on scans of retinal blood vessels in the eye,[44] hand geometry, and fingerprint identification. In addition, there are currently three classes of physiological-behavioral identification systems based on voice identification, keystroke rhythm, and signature dynamics. Most systems incorporate adaptive algorithms to track slow variations in users' physical or behavioral characteristics. Although these adaptive features reduce the rate of false rejections, some can be exploited by imposters. Most systems also allow the preset factory threshold levels for acceptance and rejection to be adjusted by the user. Tables 5 and 6 illustrate some of the characteristics of biometric and behavioral technologies.

Biometrics is currently in a state of flux: technologies are advancing rapidly, firms are entering and leaving the marketplace, and new products are being tested and introduced. These technologies are being developed and marketed by a relatively large group of firms—28 at the end of 1986—some are backed by venture capital, and some are divisions of large multinational corporations. Many other companies were doing preliminary work in biometric or behavioral techniques. Therefore, these tables and the following discussions of biometric identification systems represent only a snapshot of the field.

There is evidence of growing interest in biometrics on the part of some Federal agencies. According to *Personal Identification News*, defense and intelligence agencies conducted more than 10 biometric product evaluations in 1986.[45]

Retina Blood Vessels

Retina-scanning technology for personal identification is based on the fact that the pattern of blood vessels in the retina is unique for each individual. No two people, not even identical twins, have exactly the same retinal vascular patterns. These patterns are very stable personal characteristics, altered only by serious physical injury or a small number of diseases, and are thus quite reliable for biometric identification. Factors such as dust, grease,

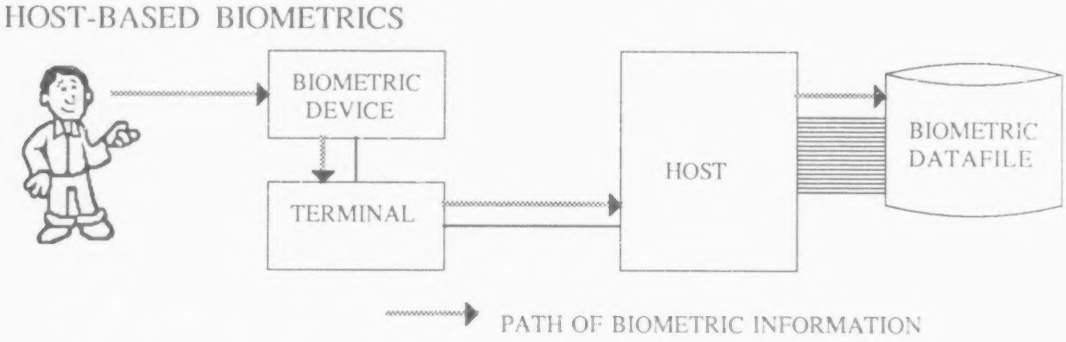
---

[43] Robert G. Anderson, David C. Clark, and David R. Wilson, "See-Through Security," *MIS Week*, Apr. 7, 1986.

[44] According to *Personal Identification News*, February 1987, a patent has been issued for another type of eye system based on measurements of the iris and pupil (Leonard Flom and Aron Safir, U.S. Patent 4,641,349, Feb. 3, 1987).

[45] *Personal Identification News*, January 1987, p. 2.

Figure 20.—Biometric Identification Configuration Alternatives: Host-Based v. Stand-Alone



Description of authentication session

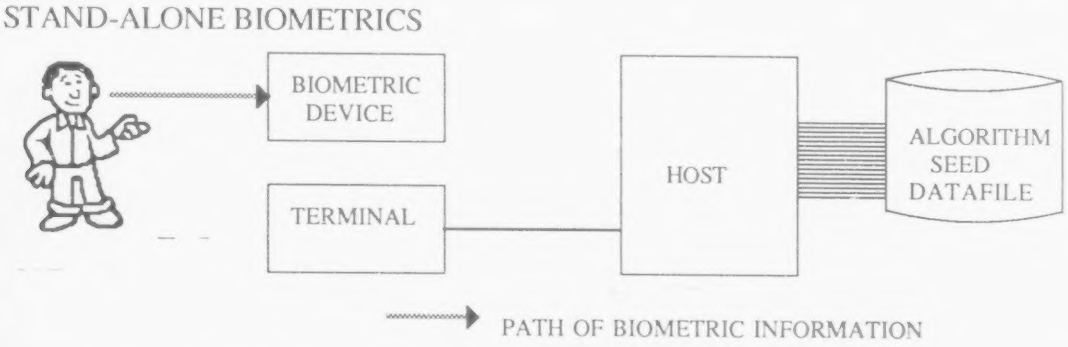
The user requests host access through the terminal, and enters his user ID. The host requests biometric authentication. The user enters the biometric information into the biometric device. The biometric data is transmitted to the host, where it is compared with the biometric data on file in the biometric datafile. Access is granted or denied.

Pros:

The user can gain access through any biometric device connected to the appropriate host. The device can be associated with terminals instead of users. An organization may require fewer devices in this mode, and the devices do not need to be portable.

Cons:

The biometric information can be compromised in transmission or storage. Encrypted information can be diverted and attacked cryptologically.



Description of authentication session

The user requests host access through the terminal, and enters his user ID. The host calculates a random challenge and sends the challenge to the user terminal. The user identifies himself to the biometric see-through device through biometric input. The user then enters the random challenge into the device. The device calculates a response based on the algorithm and the user's algorithm seed. The user enters the response into the terminal for transmission to the host. The host performs the same calculations, obtaining the user's algorithm seed from the algorithm seed data file, and compares the responses. Access is granted or denied.

Pros:

No transmission or remote storage of the biometric information is required; the information is only maintained locally in the device itself. Also, the device does not need to be designed for connection to any particular terminal.

Cons:

Individual biometric devices are needed for each user, and the devices must be portable. This could result in an expensive implementation. Also, administrative issues may be more difficult to resolve in the stand-alone configuration. For example, a device malfunction may result in access denied to a user; in the host-based configuration, the user would gain access through an alternate device.

SOURCE: Ernst & Whinney, prepared under contract to OTA, November 1986.

Table 5.—Major Characteristics of Automated Biometric Identification Types

	Eye retinal	Finger print	Hand geometry	Voice	Keystroke	Signature
Stability of measure (period)	Life	Life	Years	Years	Variable	Variable
Claimed odds of accepting an imposter (technically achievable without a high rate of false rejections)	1 in billions	1 in millions	1 in thousands	1 in thousands	1 in a thousand	1 in hundreds
Ease of physical damage—sources of environmentally caused false rejects	Difficult—a few diseases	Happens—cuts, dirt, burns	Happens—rings, swollen fingers or joints, sprains	Happens—colds, allergies, stress	Happens—emotions, fatigue, learning curve for device	Happens—stress, position of device
Perceived intrusiveness of measure	Extreme to a small portion of population	Somewhat	Modest	Modest	None	Modest
Privacy concerns: surreptitious use of measure	Not feasible to do a scan surreptitiously	Data base can be compared to law enforcement files	Not a problem	Measurement can be transparent to user	Measurement can be transparent to user	Behavior is already recognized as an ID function
Intrapersonal variation (chance of a false rejection, given training and experience in use)	Low	Low	Low	Moderate	Moderate	Moderate
Size of data template on current units	35 bytes	Several hundred to several thousand bytes	18 bytes to several hundred bytes	Several hundred bytes	Several hundred bytes	50 bytes to several hundred bytes
Throughput time (note: level of security affects processing time)	2 to 3 seconds	4 to 5 seconds	3 to 4 seconds	3 to 5 seconds	Continuous process	2 to 5 seconds
Cost range of products on the market (depends on configuration)	$6,000 to $10,000	$3,500 to $10,000	$2,800 to $8,000	$1,500 to $5,000 per door	$250 per terminal and up	$850 to $3,500
Development goal for cost per workstation (by 1990)	$2,000	$2,000	$500 to $1,000	$100 to $250	$100 to $750	$300 to $500
Approximate number of patents outstanding	Less than 10	50	30	20 plus	Less than 10	100
Approximate number of firms in market with products or prototypes as of summer 1986 (number with prototypes in parentheses)	1 (0)	3 (5)	2 (4)	2 (4)	1 (1)	3 (4)

NOTE: Other biometric PIDs under development include wrist vein, full-face, brainwave, skin oil, and weight/gait devices.

SOURCE: Benjamin Miller, prepared under contract to OTA, October 1986. Data update as of April 1987.

Table 6.—Configurations and Applications of Biometric Devices

	Configurations				Applications			
	Off-line: reference templates stored			On-line: host data base				
	In device	On mag stripe	On I.C. card		Physical security	Computer security	Law enforcement	Financial transaction
Eye/retina	U	—	B	U	U	B	B	—
Fingerprint	D	—	U	U	U	U	U	D
Hand geometry	B	U	—	U	U	—	—	—
Voice	D	—	D	U	U	B	—	D
Keystroke dynamics	B	—	—	B	—	B	—	D
Signature	D	U	B	U	U	U	—	B

U = In regular use by industry or Government
B = In Beta test use by industry or Government
D = In Development

SOURCE: Benjamin Miller, prepared under contract to OTA, October 1986. Data updated as of April 1987

and perspiration that can make fingerprint techniques difficult do not affect retinal scanning, and injuries to the hand or fingers are more common than severe eye injuries.

At present, only one firm produces a retina-scanning identification device. One of its current models, mainly used for physical access control, was introduced in September 1984. Subjects look into an eyepiece, focus on a visual alignment target, and push a button to initiate the scan (done using low-intensity infrared light). The retinal pattern scanned is compared with a stored template and identification is based on a score that can range from -1 to $+1$, depending on the degree of match. A new, low-cost version introduced at the end of 1986, uses a hand-held unit (the size of a large paperback book). It is intended for controlling access to computer terminals.

Potential applications are varied, but early purchasers are using the system for a range of uses, from physical access control to employee time-and-attendance reporting. Installations for physical access control have included a national laboratory, banks, a state prison, office buildings, and hospital pharmacy centers. According to the trade press, 300 units of the system had been shipped to end-users, original equipment manufacturers, and dealers by early 1986.[46] Some overseas users are also beginning to order the systems.

While retina scanning is fast, accurate, and easy to use, anecdotal reports suggest that the technique is perceived as being personally more intrusive than other biometric methods. Nevertheless, at the end of 1986, retinal technology accounted for the largest installed base of biometric units.[47]

Hand Geometry

Several techniques for personal identification using aspects of hand geometry were under development or in production as of early 1986. First developed in the 1970s, more than 200 hand geometry devices are in use nationwide.

The oldest hand geometry technique was based on the length of fingers and the thickness and curvature of the webbing between them. Other techniques use the size and proportions of the hand or the distances between the joints of the fingers, infrared hand topography, palm print and crease geometry, or transverse hand geometry (viewing the sides of the fingers to measure hand thickness as well as shape). Some of these techniques combine the biometric measurement with a personal identification number. The biggest measurement problems with these devices involve people who wear rings on their fingers or whose fingers are stubbed or swollen.

The use of hand geometry systems was limited initially to high-security installations because of the cost and physical size of the equipment. However, technological advances have lowered equipment cost and size, thus extending the market to medium-security facilities, such as banks, private vaults, university food services, and military paycheck disbursing. According to vendors, users include insurance companies, a jai alai facility, engineering firms, and corporate offices. At the same time, more sophisticated systems being developed for high-security areas, such as military and weapons facilities, use a television camera to scan the top and side of the hand.

---

[46] *Personal Identification News*, April 1986.

[47] *Personal Identification News*, January 1987, p. 3.

Fingerprints

Fingerprints have been used to identify individuals since the mid-1800s.[48] Manual fingerprint identification systems were based on classifying prints according to general characteristics, such as predominant patterns of loops, whorls, or arches in the tiny fingerprint ridges, plus patterns of branches and terminations of the ridges (called minutiae). Fingerprint file data were obtained by using special ink and a ten-print card; fingerprint cross-checking with local and national records was done manually. The cross-checking process began to be automated in the late 1960s and by 1983 the Federal Bureau of Investigation (FBI) had converted all criminal fingerprint searches from manual to automated operations.[49] Some State and local law enforcement agencies are also beginning to automate their fingerprint records at the point of booking.

Several firms sell fingerprint-based systems for physical access control or for use in electronic transactions. The systems generally operate by reading the fingerprint ridges and generating an electronic record, either of location of minutia points or as a three-dimensional, terrain-like image. The scanned live print is compared with a template of the user's prerecorded print. The user is verified if the recorded and live print match within a predetermined tolerance. Alternative modes of operation use an individual password, identification number, or a smart card carrying the template fingerprint data. Costs vary according to the system configuration, but they are expected to fall rapidly as more systems are sold and as very large scale integrated (VLSI) technology is used.

By mid-1986, about 100 fingerprint-based systems had been installed, mostly in high-security facilities where physical access or sensitive databases must be reliably controlled. Some units, however, have been installed in health clubs, banks, and securities firms, either to control access or for attendance reporting. Also, firms are beginning to find overseas markets receptive. Potential applications will be wider as the price and size of the systems decrease. The bulk of near-term applications are expected to be mainly for physical access control, but work station devices are progressing.

Voice Identification

Subjective techniques of voice identification —listening to speakers and identifying them through familiarity with their voices—have been admissible evidence in courts of law for hundreds of years.[50] More recently, technical developments in electronics, speech processing, and computer technology are making possible objective, automatic voice identification, with several potential security applications and important legal implications.[51] The sound produced by the vocal tract is an acoustic signal with a phonetic and linguistic pattern that varies not only with the speaker's language and dialect, but also with personal features that can be used to identify a particular speaker.

---

[48] For a complete discussion of fingerprint identification techniques, see: "Fingerprint Identification," U.S. Department of Justice, Federal Bureau of Investigation (nd); and *The Science of Fingerprints*, U.S. Department of Justice, Federal Bureau of Investigation, (Washington, DC: U.S. Government Printing Office, Rev. 12/84).

[49] Charles D. Neudorfer, "Fingerprint Automation: Progress in the FBI's Identification Division," *FBI Law Enforcement Bulletin*, March 1986.

[50] Historical and theoretical discussion of voice identification and its legal applications can be found in: Oscar Tosi, *Voice Identification: Theory and Legal Applications* (Baltimore, MD: University Park Press, 1979).

[51] Although courts in several jurisdictions have ruled that voiceprints are scientifically unreliable, courts in some States, including Maine, Massachusetts, and Rhode Island, consider them to be reliable evidence. A recent ruling by the Rhode Island Supreme Court allowed a jury to consider evidence of voiceprint comparisons and to decide itself on the reliability of that evidence, noting that, "The basic scientific theory involved is that every human voice is unique and that the qualities of uniqueness can be electronically reduced . . ." (*State* v. *Wheeler*, 84-86-C.A., July 29, 1985). Source: *Privacy Journal*, August 1985, p. 2.

Voice recognition technology has been around for some time,[52] but personal identification systems using it are just beginning to reach the market, mainly because of the formerly high cost and relatively high error rates.[53] Some large electronics and communications firms have experimented with voice recognition systems for many years, but are just now developing systems to market.[54]

An important distinction should be made here between technologies to understand words as spoken by different individuals (speech recognition) and technologies to understand words only as they are spoken by a single individual (speech verification). Voice identification systems are based on speech verification. They operate by comparing a user's live speech pattern for a preselected word or words with a pre-enrolled template. If the live pattern and template match within a set limit, the identity of the speaker is verified. Personal identification numbers are used to limit searching in the matching process. According to manufacturers and industry analysts, potential applications include access control for computer terminals, computer and data-processing facilities, bank vaults, security systems for buildings, credit card authorization, and automatic teller machines.

Signature Dynamics

A person's signature is a familiar, almost universally accepted personal verifier with well-established legal standing. However, the problem of forgery—duplicating the appearance of another person's signature—raises substantial barriers to the use of static signatures (i.e., recognizing the appearance of the signed name) as a secure means of personal identification.

Newer signature-based techniques use dynamic signature data that capture the way the signature is written, rather than (or, in addition to) its static appearance, as the basis for verification. The dynamics include the timing, pressure, and speed with which various segments of the signature are written, the points at which the pen is raised and lowered from the writing surface, and the sequence in which actions like dotting an "i" or crossing a "t" are performed. These actions are very idiosyncratic and relatively constant for each individual, and are very difficult to forge.[55]

A number of companies have researched signature dynamics over the past 10 years and several have produced systems for the market. The systems consist of a specially instrumented pen and/or a sensitive writing surface. Data are captured electronically and processed using proprietary mathematical algorithms to produce a profile that is compared with the user's enrolled reference profile or template. The systems work with an identification number or smart card identifying the profile and template to be matched.

Prices for these systems are relatively low compared with some other identification technologies. Combined with the general user acceptability of signatures (as opposed, say, to fingerprinting or retinal scans), this is expected to make signature dynamics suitable for a wide range of applications.[56] Potential financial applications include credit card transactions at the point of sale, banking, automatic teller machines, and electronic fund transfers. Systems are currently being tested in banking (check cashing) and credit card applications, where they might eventually replace dial-up customer verification systems.[57] Systems connected to a host computer could also provide access control as well as accountability and/or authorization for financial transactions and controlled materials, among other uses.

---

[52] The basics of most voice systems can be traced to work over the past 20 years at AT&T Bell Laboratories. *Personal Identification News*, October 1985.

[53] See Tosi, "Fingerprint Identification," U.S. Department of Justice, Federal Bureau of Investigation (nd); and *The Science of Fingerprints*, U.S. Department of Justice, Federal Bureau of Investigation (Washington, DC: U.S. Government Printing Office, Rev. 12/84), ch. 2.

[54] Personal Identification News, January 1986.

[55] Several signature dynamics systems have adaptive features that can allow a person's signature to vary slowly over time; enrollment procedures require several signatures to set the reference signature profile and users are permitted more than one (usually two) signature attempts for identification.

[56] George Warfel, "Signature Dynamics: The Coming ID Method," *Data Processing and Communications Security*, vol. 8, No. 1. (n.d.)

Keyboard Rhythm

Early work, beginning in the 1970s, on user verification through typing dynamics was done by SRI International and, with National Science Foundation (NSF) funding, the Rand Corp.[58] In 1986, two firms were developing commercial personal identification systems based on keyboard rhythms for use in controlling access to computer terminals or microcomputers, including large mainframe computers and computer networks. One of the firms acquired the keystroke dynamics technology from SRI International in 1984 and contracted with SRI to develop a product line. In 1986, the firm reported that it was developing 11 products configured on plug-in printed circuit boards and that it planned to test these products in several large corporations and Government agencies in 1987. By mid-1987, the firm had contracts with over a dozen Fortune 500 corporations and five Government agencies to test its products.[59] A researcher in the second firm, who had received an NSF grant in 1982 to investigate typists' "electronic signatures," formed a venture corporation in 1983 to commercialize an access control device based on the technique. He was awarded a patent in late 1986.

Keyboard-rhythm devices for user verification and access control are based on the premise that the speed and timing with which a person types on a keyboard contains elements of a neurophysiological pattern or signature that can be used for personal identification.[60] The stored "user signature" could be developed explicitly or so that it would be transparent to the user—perhaps based on between 50 and 100 recorded log-on accesses or 15 to 45 minutes of typing samples if done openly and explicitly, or based on several days of normal keyboard work if done transparently (or surreptitiously). The stored signature could be updated periodically to account for normal drifts in keyboard rhythms. These types of devices might be used only at log-on, to control access to selected critical functions, or to prevent shared sessions from occurring under one user log-on. The prices of these systems depend on their configuration: current estimates range from $1,000 for a card insert for a host computer capable of supporting several work stations to $10,000 for a base system that could store 2,000 user signature patterns and support four channels that communicate simultaneously.

---

[57] Ibid.

[58] R. Stockton Gaines, William Lisowski, S. James Press, and Norman Shapiro, "Authentication by Keystroke Timing: Some Preliminary Results," R-2526-NSF, The RAND Corp., Santa Monica, CA, May 1980.

[59] Rob Hammon, International Bioaccess System Corp., personal communications with OTA staff, Aug. 4, 1987.

[60] Some speculate that this method would only be effective for experienced typists, rather than erratic "hunt and peck" novices, but at least one of the firms claims that the method can be implemented for use by slow or erratic typists as well.

ACCESS CONTROL SOFTWARE AND AUDIT TRAILS

Once the identity of a user has been verified, it is still necessary to ensure that he or she has access only to the resources and data that he or she is authorized to access. For host computers, these functions are performed by access control software. Records of users' accesses and online activities are maintained as audit trails by audit software.

Host Access Control Software

To provide security for computer systems, networks, and databases, user identifications and passwords are commonly employed with any of a number of commercially available add-on software packages for host access control. Some have been available since the mid-to-late

Box D.—Host Access Control Software

A number of host access control software packages are commercially available that work with a computer's operating system to secure data and the computing resources themselves. Access control sofware is designed to offer an orderly method of verifying the access authority of users. As such, it can protect the system, its data, and terminals from unauthorized users and can also protect the system and its resources from unauthorized access to sensitive data and from errors or abuses that could harm data integrity.

Access control software intercepts and checks requests for system or database access; the various commercial packages vary in the ways they check requirements for authorized access. Most require both user identification and a password to allow access; the user's identification determines his or her level of access to the system hardware and files. Passwords may be changed from time to time, or even (in some systems) encrypted. To prevent unauthorized users from guessing passwords, most of these systems limit the number of incorrect access attempts before logging the user off and sending a security alert message (including the user's identification number). Some packages generate their own passwords; these tend to be more difficult for intruders to guess, but also are more difficult for authorized users to remember. The data files containing user identification numbers and passwords are critical to system security because knowledge of correct identification number and password combinations would allow anyone access to the system and its most sensitive files. Therefore, some access control packages do not allow even security administrators to know user passwords—users set up their own, or the system generates the passwords, which may change frequently. The structure of system-generated passwords is being studied to make them easier to remember.

Access control software packages allow for audit features that record unauthorized access attempts, send violation warning messages to security, and/or log the violator off the system. Other audit features include keeping a log of users' work activities on a daily basis, printing reports of use and violation attempts, and allowing security officers to monitor users' screens. These packages can also be used in conjunction with special facility-specific security access controls implementing other restrictions (time-of-day, database, file, read-only, and location/terminal) written in custom code to fit the application environment. Versions of access control software packages are currently available to protect a variety of manufacturers' mainframe operating systems and minicomputers.

Development of software for commercial host access control began in the early 1970s. Currently, there are more than 24 software packages from different vendors. These packages are designed to work with a variety of host configurations (CPU, operating system, storage space, interfaces to other system software).

SOURCE: DataPro Research Corp., "All About Host Access Control Software," IS52-001, June 1985.

1970s. (See box D.) As of 1986, three access control software packages were market leaders: RACF, with some 1,500 installations since 1976; ACF2, developed by SKK, Inc., and marketed by the Cambridge Systems Group, with more than 2,000 installations since 1978; and Top Secret, marketed by the CGA Software Products Group, with more than 1,000 packages installed since 1981.[61]

In all, more than two dozen software packages are being marketed, some for classified applications. These packages vary widely in their range of capabilities and applications, and are usually either licensed with a one-time fee or leased on a monthly or yearly basis. Fees and maintenance can range from several hundred dollars up to $50,000 per year.

Instead of the "add-on" software packages mentioned above, the operating systems of many computers include some level of access control built into the basic system software. Most of the built-in systems offer features comparable to the add-on systems designed for commercial use.[62] The number of new computer operating systems incorporating access control and other security features is expected to increase.

---

[61] DataPro, reported in *Government Computer News*, Dec. 5, 1986, p. 40.

Commercial access control software packages commonly rely on users memorizing their identification numbers or passwords keyed into the terminal. Thus, they tend to rely on the "something known" criterion for security. They also tend to permit a single individual—in principle, the security officer—access to the central files containing users' authorization levels and, although less prevalent in newer systems, their users' passwords. A characteristic of the higher security packages is that they are designed for applications in which users with varying levels of authorization are using a system containing information with varying degrees of sensitivity. An example is a system containing classified information, where some is classified "confidential" and some "secret."

NSA's National Computer Security Center (NCSC) has provided Federal agencies with criteria to evaluate the security capabilities of trusted computer systems. According to the NCSC definition, a trusted computer system is one that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information. The trusted system criteria contained in the so-called "Orange Book,"[63] developed by NSA, define four classes of security protection. These range from Division D (minimal protection) up through Class A1 of Division A (verified protection). NCSC also evaluates access control software products submitted by vendors and rates them according to the Orange Book categories. The evaluations are published in the Evaluated Products List, which is made available by NCSC to civilian agencies and the public. As of May 1987, eight products had received NCSC ratings and more than 20 others were being evaluated.

Despite their importance to host computer security, particularly for classified applications, a detailed look at trusted operating systems is beyond the scope of this OTA assessment. A number of computer security experts, including those at NSA, consider trusted operating systems to be crucial to securing unclassified, as well as classified, information. They consider access controls to be of limited value without secure operating systems and the NCSC criteria, at least at the B and C levels, to be of significant value in both classified and commercial applications.[64] However, other computer security experts have questioned whether design criteria appropriate for classified applications can or should be applied to commercial applications or even to many unclassified Government applications. (See ch. 5.)

The recent debate over the applicability of what some term the "military" model to commercial computer security[65] had progressed to the point where plans were made for an invitational workshop on this topic to be held in the fall, 1987.[66] This specific area of concern illustrates the issue of whether or not it is in the Nation's best interests to assign to one agency—namely, NSA—the task of meeting all the needs of the Government's civilian agencies and the private sector while continuing to carry out its other missions. These concerns will be raised again and explored in chapters 5 and 7.

---

[62] S. Lipner, personal communication with OTA staff, Dec. 24, 1986.

[63] Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense Standard DoD 5200.28-STD, December 1985. Two companion DoD documents ("Yellow Books") summarize the technical rationale behind the computer security requirements and offer guidance in applying the standard to specific Federal applications: *Computer Security Requirements—Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, CSC-STD-003-85, June 25, 1985; and *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements*, CSC-STD-004-85, June 25, 1985.

[64] Harold E. Daniels, Jr., NSA S-0022-87, Jan. 21, 1987. Safeguards currently used by the private and civil sectors have received B- and C-level ratings.

[65] See, for example, David D. Clark and David R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," *Proceedings, 1987 IEEE Symposium on Security and Privacy* (Oakland, CA: Institute for Electrical and Electronic Engineers, Apr. 27-29, 1987).

[66] The Workshop on Integrity Policy for Computer Information Systems will be held at Bentley College, Waltham, MA in the fall, 1987. It is being organized by Ernst & Whinney, and is co-sponsored by the Association for Computing Machinery, the Institute for Electrical and Electronic Engineers, the National Bureau of Standards, and the National Computer Security Center.

Audit Trails

Another major component of computer security, usually part of a host access control system, is the ability to maintain an ongoing record of who is using the system and what major actions are performed. The system's operators can then review this "audit trail" to determine unusual patterns of activity (e.g., someone consistently using the system after office hours) or to reconstruct the events leading to a major error or system failure.

In the past few years, software has begun to combine auditing with personal identification. An audit log can record each time a user seeks access to a new set of data. Figure 21 shows a sample audit log. Audit trail software is routinely recorded on most mainframe computers that have many users. Such software is available but seldom used on similar minicomputers, in part because it slows down the performance of the system and is only rarely available for microcomputers.

Audit trails are among the most straightforward and potentially most effective forms of computer security for larger computers and multi-user minicomputers. However, the fact that they are easily available for these machines does not mean that they are effectively used. Many system managers either do not use the audit trails or rarely if ever review the logs once generated. For example, OTA found that only 58 percent of 142 Federal agencies surveyed use audit software for computers containing unclassified, but sensitive information. Only 22 percent use audit software for all of their unclassified, but sensitive systems.[67] Similarly, a 1985 General Accounting Office (GAO) study that examined 25 major computer installations found that only 10 of them met GAO's criteria for use of audit trails.[68]

Part of the reason why audit trails are not more widely and effectively used is that they tend to create voluminous information that is tedious to examine and difficult to use. Technical developments can ease this problem by providing tools to analyze the audit trail information and call specified types or patterns of activities to the attention of system security officers. Thus, it would not be necessary, except in case of a disaster, to review the entire system log.

ADMINISTRATIVE AND PROCEDURAL MEASURES

Important as technical safeguard measures like the ones that have been described above can be, administrative and procedural measures can be even more important to overall security. For example, encryption-based communications safeguards can be rendered useless by improper management of "secret" encryption or decryption keys (see below). In the field of computer security, technical measures of the types mentioned above are almost useless if they are not administered effectively. While they can only be raised briefly here, some

---

[67] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems To Unauthorized Access," OTA contractor report, November 1986.

[68] William S. Franklin, General Accounting Office, statement on Automated Information System Security in Federal Civilian Agencies, before House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, 99th Cong., 1st. sess., Oct. 29, 1985.

Figure 21.—Example Reports From Audit Trail Software

```
Example 1
=========
Security alarm / System UAF record modification
        Time:             27-OCT-1986 08:43:09.49
        PID:              00002420
        User Name:        SYSTEM
        Rec Mod:          SMITH
        Fields Mod:       PASSWORD        PRIVILEGES

Example 2
=========
Security alarm / File access failure
        Time:             27-OCT-1986 11:11:15.76
        PID:              00002402
        User Name:        JONES
        Image:            DUA0:[SYS0.][SYSEXE]TPU.EXE
        File:             _DUA1:[DESNC.PH2]DOCS.DIR;1
        Mode:             READ WRITE


Example 3
=========
Security alarm / Login failure
Username:          GUEST             UIC:                   [1,3]
Account:           <net>             Finish time:           25-DEC-1986 12:28:48.
Process ID:        00000573          Start time:            25-DEC-1986 12:28:47.
Owner ID:                            Elapsed time:                    0 00:00:00.
Terminal name:                       Processor time:                  0 00:00:00.
Remote node addr:  36000             Priority:              4
Remote node name:  APPLE             Privilege <31-00>:     FFFFFFFF
Remote ID:         BANANA            Privilege <63-32>:     FFFFFFFF
Queue entry:                         Final status code:     00D380F4
Queue name:
Job name:
Final status text: %LOGIN-F-NOSUCHUSER, no such user
Page faults:                114      Direct IO:                       8
Page fault reads:             2      Buffered IO:                     9
Peak working set:           144      Volumes mounted:                 0
Peak page file:             534      Images executed:                 1
No files accessed through [DECNET]

--------------------------------------------------------------------------
```

Audit trail software (either part of the computer's operating system or an add-on program) can record in detail the activities taking place on a computer system. The first example above reports a manager ("SYSTEM") modifying a user's ("SMITH") password and privileges (the activities that user is allowed to perform on the system). The second records a user ("JONES") attempting to access a file for which he does not have privileges. The third reports someone trying to log in to a system under the name "GUEST," which is not an authorized user of that system. A typical audit trail program might produce hundreds to thousands of these reports in a day.

SOURCE: Digital Equipment Corp., 1986.

of the most important aspects of computer security administration include:[69]

- *Maintaining a Written Security Policy and Assigning Responsibilities for Security.* Many organizations simply do not have a policy regarding computer security, or the policy is unavailable to computer users, or the policy is not followed. Computer security experts report that one of the most important factors in encouraging good computer security is for users to know that management is indeed committed to it. Also, it is important that each individual in the organization be aware that protecting information assets is part of his or her responsibility.
- *Password Management.* Password-based access control systems are much less effective if computer users write their passwords on the wall next to their terminal, if they choose their birthday or spouse's name as their password, or if passwords are never changed. Thus, policies to encourage reasonable practices in password systems are not only essential, but are probably one of the simplest and most neglected ways to enhance security.
- *Reviewing Audit Trails.* Similarly, audit software is of little value unless the logs created by its use are reviewed.
- *Training and Awareness.* Relatively simple programs can help users understand what kind of security problems the organization faces and their role in enhancing security.
- *Periodic Risk Analyses.* Such an analysis involves examining each computer system, the sensitivity of the data it handles, and the measures that are in use or should be considered to protect the system.
- *Personnel Checks.* Organizations may wish to avoid putting employees with certain kinds of criminal records or financial problems in jobs with access to sensitive information. It may be difficult, however, to perform such checks without raising concerns about employee privacy.
- *Maintaining Backup Plans and Facilities.* Many organizations do not have any policy or plans for what to do in the event of a major disaster involving an essential computer system. For example, in 1985 only 57 percent of Federal agencies had (or were in the process of developing) backup plans for their mainframe computer systems.[70]

COMPUTER ARCHITECTURES

The computer itself has to be designed to facilitate good security, particularly for advanced security needs. For example, it should monitor its own activities in a reliable way, prevent users from gaining access to data they are not authorized to see, and be secure from sophisticated tampering or sabotage. The national security community, especially NSA, has actively encouraged computer manufacturers to design more secure systems. In particular, NCSC has provided guidelines for secure systems and has begun to test and evaluate products submitted by manufacturers, rating them according to the four security divisions discussed above. A more thorough discussion of secure computing bases is beyond the scope of this assessment.

While changes in computer architecture will gradually improve security, particularly for larger computer users, more sophisticated architecture is not the primary need of the vast majority of current users outside of the national security community. Good user verification coupled with effective access controls, including controls on database management systems, are the more urgent needs for most users.

---

[69] For a more complete discussion of administrative procedures for computer security, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight,* OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986). Additionally, the General Accounting Office (GAO) has issued many reports over the last decade identifying major information security problems and surveying information security practices in Federal agencies (see tables 4-5 in the February 1986 OTA report for a selected list of some of these GAO reports).

[70] Data from OTA's Federal Agency Request given in ch. 4 of *Federal Government Information Technology: Management, Security, and Congressional Oversight,* OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986).

COMMUNICATIONS LINKAGE SAFEGUARDS

In the past few years it has become increasingly clear that computers are vulnerable to misuse through the ports that link them to telecommunications lines, as well as through taps on the lines themselves. Although taps and dial-up misuses by hackers may not be as big a problem as commonly perceived, such problems may grow in severity as computers are increasingly linked through telecommunications systems. Similarly, computer and other communications using satellite transmissions motivate users to protect these links.

Port-Protection Devices

For some computer applications, misuse via dial-up lines can be dramatically reduced by the use of dial-back port protection devices used as a buffer between telecommunications lines and the computer. The market for these is fairly new, but maturing. Some products are stand-alone, dial-back units, used for single-line protection; others are rackmounted, multiline protection units that can be hooked up to modems, telephones, or computer terminals. Some 40 different models of commercial dial-back systems were being sold in 1986, with prices ranging from several hundred to several thousand dollars (on the order of $500 per incoming line), depending on the configuration, features, and number of lines protected. Some, but not all, models offer data encryption as a feature, using DES and/or proprietary algorithms.

In addition to these dial-back systems, security modems can be used to protect data communications ports. These security modems are microprocessor-based devices that combine features of a modem with network security features, such as passwords, dial-back, and/or encryption. Security modems featuring encryption must be used in pairs, one at each end with the correct encryption key and algorithm to encrypt and decrypt communicated data and instructions. About 20 different models of commercial security modems were available in 1986, with various combinations of features, such as password protection, auditing, dial back, and/or encryption. Security modems featuring encryption offer the DES and/or proprietary encryption algorithms.

According to DataPro Research Corp., the market for security modems has been in a period of rapid change since the early 1980s—new and advanced products have been introduced, more users have adopted remotely accessible data operations, and prices have continued to fall. Prices for security modems range from less than $500 to almost $2,000, depending on the features included.

An example of the use of this type of port protection follows: When a remote user wants to log on to the machine, the security modem is programmed to answer the call, ask for his or her log-on identification and password, and then (if the identification and password are proper) call back the computer user at the location at which he or she is authorized to have a terminal. There may be some inconvenience in using the device, however, if authorized computer users frequently call from different phone numbers. In addition, there are ways to thwart dial-back modems, such as using "call-forwarding" at the authorized user's phone to route the computer transmission elsewhere to an unauthorized phone or user.

Dial-back devices are generally considered too inconvenient to use for one very important application: large-scale database applications, such as commercial credit reporting services. These services can receive thousands of calls a day from terminals in banks and credit bureaus seeking to verify a person's credit worthiness, often prior to a loan or establishment of a line of credit. The use of dial-back devices for such an application are time-consuming and costly, and are difficult to administer given the number of terminals that would have to be connected to the devices. Thus, those who illegally obtain passwords to access these systems can now use them relatively easily.

Other technical measures may be useful for large public database systems, however. For example, remote terminals in retail stores could be equipped to perform a coded "handshake" with the host computer before they can gain access to the database. Or, as the telecommunications network evolves toward wider use of digital signaling equipment, it will increasingly be possible for host computers to know the phone number of the person trying to gain access and thus to check that phone number against its list of authorized customers.

Satellite Safeguards

In the military, highly directional antennas, spread-spectrum modulation, and laser communication are among the measures used or contemplated to protect satellite signals from unauthorized reception. Other methods range from analog scrambling to full digital encryption. For encryption, equipment costs and operational complexity tend to inhibit the widespread deployment of elaborate encryption techniques. This is particularly true for point-to-multipoint networks, where the expense of providing a large number of end users with decryption equipment may not be worth the cost.

The current trend is toward the implementation of security by some service providers. For example, the video industry, one of the largest users of satellite capacity, has begun to use analog scrambling techniques to discourage casual theft of service. Methods for encrypting video signals range in complexity from line-by-line intensity reversal to individual pixel scrambling. Decryption keys may be broadcast in the vertical blanking interval. In some systems, individual subscribers can be addressed, providing selective access to the programming. Scrambling techniques are also being used by some providers of point-to-multipoint satellite data networks. Since these transmissions are typically digital, more effective encryption systems can be used. In some cases, a device using the Data Encryption Standard is provided in the subscribers' receiver equipment and key distribution is accomplished in real time to selected end users (i.e., to those who have paid to receive the broadcast).[11]

The Department of Defense has had continuing concerns for the vulnerability of satellites to interception and other misuse. The Senate Committee on Appropriations approved funds in 1986 for the first year of a 5-year plan developed by NSA that would enable DoD to reimburse satellite carriers for installing encryption equipment to protect their transmissions.[12]

Fiber Optic Communications

Fiber optic communications links provide an important barrier to misuse, because more sophisticated means are required to eavesdrop. Further, means are available to detect some forms of misuse.

Common Carrier Protected Services

Several common carriers encrypt their microwave links in selected geographic areas as well as their satellite links that carry sensitive Government communications. These protected services are largely the result of NSA and GSA procurements beginning in the 1970s. Much of the following discussion is excerpted from the OTA contractor report, "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," prepared by Information Security Incorporated, November 10, 1986.

---

[11] Note that the Electronic Communications Privacy Act of 1986 (Public Law 99-508) made the private use of "backyard" earth stations legal for the purpose of receiving certain satellite transmissions, unless it is for the purpose of direct or indirect commercial advantage or for private gain.

[12] See U.S. Senate, Committee on Armed Services, National Defense Authorization Act for Fiscal Year 1987, Report 99-331 to accompany S. 2638, 99th Cong., 2d sess., July 8, 1986, p. 295.

The latest transmission technology using fiber optics is difficult to intercept because the information signal is a modulated light beam confined within a glass cable. NSA judges both cable and fiber media to provide adequate protection for unclassified national security-related information.

American Telephone & Telegraph Co. (AT&T) protects its microwave links in Washington, D.C., New York, and San Francisco. Major routes are being expanded with fiber optics. Protected service is available in areas designated by NSA and private line service can be offered over selected fiber and cable routes. In addition, customized encryption can be installed on selected microwave and satellite circuits for particular customers.[73]

MCI offers protected terrestrial microwave services in those areas specified by NSA. In addition, MCI offers customers the option of protected service in many other major metropolitan areas. These customers can order protected communications throughout the MCI portion of the circuit, using MCI's fiber optic system, encrypted terrestrial microwave, and the MCI-encrypted satellite network.[74]

U.S. Sprint, which reached 2.5 million customers or about 4 percent of all long-distance customers in 1986, intends to create an all-fiber network by the end of 1987 that the company expects will carry more than 95 percent of its voice and data traffic.[75] This means any call or circuit carried via the Sprint network would be harder to intercept than unprotected microwave transmissions. Currently, Sprint has protected microwave radio in the NSA-designated areas.[76]

International Telephone & Telegraph Co. (ITT) offers protected service in the NSA-designated zones, consisting of protected microwave circuits. The service is available now on a private-line basis to commercial or business customers.[77]

The American Satellite Co. offers two types of protected carrier services. One uses an encrypted satellite service that has been approved by NSA for protecting unclassified, but sensitive information. The second service uses protected terrestrial microwave in the NSA-designated areas. This also is available on a private line basis in the service areas.[78]

Pacific Bell plans to have a complete fiber and cable network between all its central offices within 10 years. These plans include most of San Francisco, Los Angeles, and San Diego; at present, two fiber rings in San Francisco are routed past all major office buildings. Pacific Bell can offer customers in the San Francisco area fiber optic routes throughout most of their operating region. In Los Angeles, the company has 27 locations used in the 1984 Olympics linked by fiber optic facilities and is extending its network. These offerings can be augmented with new fiber spurs to a customer's location. All of these services are filed with the California Public Utility Commission as special service engineering and are not tariffed by the FCC.[79]

Bell Communications Research (Bellcore) is developing a service that would be implemented by the Bell Operating Companies. The service would provide special handling and routing over protected or less-interceptable (i.e., fiber or cable) lines. The initial goal is to use as much as possible the inherent security features of the existing network. This service is being designed to meet NSA requirements for protecting unclassified government information so that costs (for Government contractors) will be reimbursable under National COMSEC Instruction 6002 and Department of Defense Instruction 5210.74. Bellcore anticipates that this service will also be available to other commercial customers.[80]

---

[73] AT&T Communications Security, marketing literature, 1986.

[74] MCI Communication Protection Capabilities, marketing literature, 1986.

[75] U.S. Sprint, "Clearline," vol. 2, Issue 5, Kansas City, MO, spring 1987.

[76] "Why U.S. Sprint Is Building the First Coast-to-Coast Fiber Optic Network and What's in It for You," U.S. Sprint marketing literature, 1986.

[77] ITT Private Line Service—Security, marketing literature, 1986.

[78] Protected Communications Services, marketing literature, 1986.

[79] OTA Federal Agency Data Request, op. cit.

[80] Ibid., ref. 27.

Chapter 5

Improving Information Security

CONTENTS

Page
Findings 95
Introduction 95
National Security Objectives and Programs 98
  Background 98
  Federal Telecommunications Protection Programs 98
  Government Procurements 100
  Carrier Protection Services 100
  DoD Programs Under NSDD-145 101
  Implications of Merging Defense, Civilian Agency, and Private Sector Requirements 106
Objectives and Programs Unrelated to National Security 110
  Background 110
  Private Sector Motivations 110
  Linkages in and Contrasts Between Defense-Intelligence and Other Needs 117
  Technical Standards Development 123
  Inherent Diversity of Users' Needs 127

Box

Box *Page*
E. Indicators of Private Sector Interest in Safeguards 111

Tables

Table No. *Page*
7. Overall Ranking of Importance as an Adversary 118
8. Top-Priority Computer and Information Security Concerns Mentioned by Respondents 120
9. Perceived Impacts From NSDD-145 120
10. Selected Civilian Technical Standards for Safeguarding Information Systems 126

Chapter 5

Improving Information Security

FINDINGS

- **The needs of institutional users are changing, expanding gradually and incrementally, as technology makes practical a broader range of applications of information safeguards. The current trend in user activities is toward controlling access to systems, linking transactions with particular individuals and authorizations, and verifying message accuracy.**
- **Users in civil agencies and the private sector have diverse needs to safeguard their computer and communications systems, even within any one Federal agency or industry. Organizations differ in their needs, perceptions, and attitudes towards information security, and see different incentives or mandates to secure information systems. Differences in their concerns for vulnerabilities, risks, and adversaries are probably greatest between Government intelligence agencies and other users.**
- **It is unclear whether any one agency can specify and design one or a few safeguards for a wide range of users, and particularly questionable for the National Security Agency due to its propensity for secretiveness and its focus on protecting against foreign intelligence adversaries.**
- **Cryptography underlies some powerful safeguards that have broad application, not just for national security needs, but also for an expanding number of commercial needs, such as to ensure the integrity of electronic information and reduce the costs of routine business transactions. Advances in cryptography have stimulated new nondefense applications of the technology.**
- **Federal standards and guidelines have a leveraging effect on the private sector, especially in areas related to cryptography.**
- **It is not clear how motivated the nondefense private sector will be to use some safeguards, such as secure telephones or trusted computers, particularly if these are not easy to use and cost-effective in business applications.**

INTRODUCTION

The preceding chapters illustrate the various vulnerabilities of computer and communications systems and the range of technologies that are becoming available to safeguard information in these systems. They also introduce the notion of a spectrum of adversaries, differing widely in available resources (time, money, equipment, and specialized knowledge), against whom these systems may need to be protected. This chapter examines the perceived needs of various users—defense and civilian agencies of the Federal Government, financial and other private sector users—as indicated by the actions they are taking to safeguard their domestic and international operations. It also points out some of the diversity in their perceived needs for safeguards, both among users in the private sector and, particularly, between users in intelligence agencies and others.

The level of users' activity toward safeguarding electronic information is growing. Various factors are contributing to this interest. These factors range from wanting to improve business operations, including the reduction of potential theft and human errors, to streamlining business transactions and adhering to industry standards of due care and, in some cases, to requirements imposed by emerging Federal policies. Federal policies, for example, will influence the actions of some banks and defense contractors. No individual factor is recognized as singularly prominent in driving the use of safeguards.

Instead, business uses of electronic safeguards are in a transition phase as users continue to define their needs and as technical standards are developed, and as Federal policies and agency roles stabilize further. A number of factors have complicated the situation, however. Among these is the question of the influence of the National Bureau of Standards or the National Security Agency in setting standards for information security safeguards, and users' perceptions of the prospective reach of Federal policies requiring safeguards for unclassified information. (See ch. 6.)

One important turning point appears to have been reached in that users are now better able to distinguish between the protections provided, or not provided, by different forms of safeguards and their alignment with specific needs. Users tend to be concerned with one or more of three main objectives in seeking information safeguards: preventing unauthorized disclosure; maintaining the integrity of electronic information; and ensuring continuity of service. The needs of different communities of users vary widely and these needs are often critical for one of these objectives and less important, or nonexistent, for others. For some users there is concern for all three objectives.

In spite of the difficulty in distinguishing between users according to their objectives for information security, some cautious observations can be made. One of these is that a critical need for some users, such as intelligence agencies, is to prevent unauthorized disclosure. Most businesses and civilian agencies are particularly dependent on the integrity of certain of their electronic information, and many of these are also concerned about unauthorized disclosure. And, for some users, such as those responsible for public safety (air traffic control) and many financial services, there is an important, if not critical, need for continuity of service. Observations concerning users' objectives are important because Federal policy that is misaligned with users' needs can create significant tensions.

Government agencies' and private sector needs for information security include capabilities for authenticating the origin and integrity of messages, and for verifying the identities and authorizations of system users. The Department of the Treasury and the Federal Reserve System, for example, electronically transfer huge amounts of money every working day and, with commercial banks, are providing leadership in developing and using safeguards with these types of capabilities.

Users' needs for safeguards are by no means confined to the financial community. The use of safeguards for securing electronic information is being adopted by users in industries ranging from automobile manufacturing to grocery businesses. However, private sector needs and Government national security concerns are not identical. They differ in their perceptions of the levels of adversaries, the consequences of exploitation, and their organizational motivations and decision rules for protecting information and investing in safeguard technology.[1]

In addition, private sector demand for safeguards is growing, as is its ability to produce them, as noted in chapter 4. Users tend to make selected use of a broader range of new technologies for safeguarding information that prove cost-effective or are otherwise important for business reasons. Interestingly, many of the emerging commercial uses of message integrity (authentication) techniques, e.g., for cost-reduction purposes, make use of the same cryptographic techniques used to improve the confidentiality of electronic information. Often, however, the commercial motivations for employing these techniques are unconcerned with preventing unauthorized information disclosure or protecting national security.

---

[1] Administrative and technical safeguards, as well as organizational policies for information safeguards, are also important for safeguarding electronic information, as noted in ch. 4.

What emerges is a sense that although generalizations of aggregate users' needs are useful, individual users tend to have significant diversity among them. Even within one user community, such as the banking industry, there can be considerable diversity of needs, depending on size, location, operations, clients, and numbers of branches and correspondents.

This diversity of needs raises questions with regard to the proper role of the Federal Government in meeting private sector needs and the extent to which any one Federal agency can reasonably be expected to meet the safeguard needs of all users. Such a task would require an agency to interact openly and continually with a diverse public. The intensity and openness of interaction would require significant adaptation in the operations of an agency such as DoD's National Security Agency (NSA).[2] Without a full appreciation of users' needs, there is significant risk of premature or "off-target" technology standardization or imposing DoD restrictions that are unacceptable to users. At the same time, safeguards that do not meet users' needs—even those that are federally imposed—are not likely to be applied widely and may distort market forces.

The users themselves are also likely to be important in shaping information safeguards. The influence of major international business users on information security standards is only beginning to be felt, but is likely to be significant in the long term. These users can be expected to demand safeguards that integrate well into their business operations in terms, for example, of being inexpensive, exportable, interoperable, and politically acceptable in the many countries in which the firms do business. Their influence is already beginning to be felt through communities of industry users, such as international banking, transportation, and manufacturing.

OTA analyzed survey data to gain insights into the influence of Federal policies and standards on users' and vendors' actions. Although the effects of National Security Decision Directive 145 (NSDD-145), issued in 1984, were still evolving, there were indications, as of late 1986, that the impact of this policy had not been widely felt on nongovernment users' actions. For example, about three-fourths of the nongovernment respondents to an OTA survey question, and 46 percent of the nongovernment respondents to a separate Ernst & Whinney survey, indicated that this policy had no impact on their organizations' actions toward safeguarding unclassified information.[3]

Moreover, OTA's research has found that some large firms feel that, in general, Federal guidelines and assistance programs have not significantly or directly contributed to their information security efforts.[4] Moreover, data from Ernst & Whinney's computer security survey in 1986 shows that, of 474 respondents, two-thirds said that none of their organization's information and computer security expertise came directly from Government-sponsored assistance programs, conferences, or training programs. On average, according to estimates by both government and nongovernment respondents, only 7 percent of their organizations' information and computer security expertise came directly from government programs.[5]

---

[2] See, for example, " 'Advice Most Needed . . . ' The Assessment and Advice Effort," Deborah M. Claxton, DoD. Presented at the Ninth National Computer Security Conference, Gaithersburg, MD, Sept. 18, 1986.

[3] Of 26 computer audit directors from Fortune 100 firms surveyed for OTA in October 1986, Ernst & Whinney found that 17 individuals (74 percent of the 23 answering this question) said that NSDD-145 had had "no" impact on their firms' safeguarding of unclassified information, four said NSDD-145 had had "very little" impact, and two said the directive had had "some" impact.

Results are reported in OTA contractor report, "OTA Computer Security Survey," Ernst & Whinney, Nov. 7, 1986. Ernst & Whinney included many questions from the OTA survey in a survey it conducted at the Computer Security Institute Conference in November 1986. The raw data from this Ernest & Whinney survey indicated that, of 364 nongovernment respondents, 46% said that NSDD-145 had had "no" impact, 27% "very little" impact, 21% "some" impact, and 6% "great" impact (see table 9). Ernest & Whinney has permitted OTA to use the raw data from this survey.

[4] OTA survey, October 1986, op. cit.

Vendors of information security products are especially, and understandably, sensitive to Government policies and standards that influence the use and choice of safeguards among Government agencies and businesses. The relatively small markets for many types of safeguards make any influences on consumption of these products particularly important.

The following sections examine the range of users' motivations for using safeguard technologies to protect unclassified information and spotlight what users are doing to meet their objectives. They illustrate some of the main objectives of users for safeguarding electronic information, ranging from national security to economic self-interest and the need to comply with established business practices.

For the purposes of this report, user objectives and actions are grouped into two categories:

1. those related to national security, which include a number of Federal agency actions; and
2. other Government and private sector actions not directly related to national security.

The latter category includes Federal agency actions to protect financial transactions. Attention often focuses on cryptography because it is central to many powerful safeguard techniques and because the course of technological development in cryptography-based safeguards has been so tightly meshed with Federal policies.

NATIONAL SECURITY OBJECTIVES AND PROGRAMS

Background

Traditionally, national security objectives have guided the development and use of effective information security techniques. DoD has been responsible for safeguarding classified information transmitted, stored, or processed in communications and computer systems. Recently, through NSDD-145, DoD's authority has been expanded to include protecting systems containing certain unclassified information in civilian agencies and the private sector. (See ch. 6.) This includes Government and Government-derived economic, human, financial, technological, and law enforcement information, as well as personal or proprietary information provided to the Federal Government.

Federal Telecommunications Protection Programs

Most Federal agencies have adopted some policy to protect the security of the information they collect. Issues relating to the security of Federal information systems were examined in an earlier OTA report, *Federal Government Information Technology: Management, Security, and Congressional Oversight*.[6] This section describes selected programs to protect information systems.[7]

Commercial Carrier Protection Program.—This program, begun prior to the issuance of Presidential Directive/National Security Council 24 (PD/NSC-24), involves the Nation's major telecommunications carriers. In late 1977, *The New York Times*, among other newspapers, reported that President Carter had approved a broad protection program that included routing nearly all Government telephone messages in three cities (Washington, D.C., New York, and San Francisco) through underground cable rather than over more vulnerable radio circuits.[8] At the same time, research was accelerated to improve telephone security with the long-haul, terrestrial commercial carriers. As a result, entire radio channels are now protected between switching stations in the three cities. After the technology was developed to protect the microwave radio systems, the Government began to require protected service in civil and defense agencies' communications procurements. (See ch. 6 for a description of the evolution of these communications security programs.)

---

[5] This data is from Ernst & Whinney's survey administered at the Computer Security Institute Conference on Nov. 17-20, 1986.

[6] OTA-CIT-297, February 1986. Chapter 4 of this report surveys the security of unclassified information systems within the Federal Government.

[7] Part of this section is based on material taken from chapter IV of OTA contractor report, "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," Information Security, Inc., November 1986.

Currently, 450 microwave radio channels carrying more than 1 million voice and data circuits are protected. More than 1 million sensitive telephone calls are protected each day and NSA expects that almost 2 million circuits will be protected in 1988. Although this program was prompted by defense concerns for safeguarding DoD contractor communications, defense and non-defense protection requirements were aggregated for efficient bulk or network-level protection.[9]

Secure Voice Programs.—As reported by *The New York Times* in late 1977, the Executive Secure Voice Network program was initiated to provide 100 selected Government executives and surveillance targets[10] with a total of 250 secure voice terminals at a cost of $35,000 each. The equipment, intended to secure classified information up to Top Secret Compartmented, used narrowband, dial-up telephone lines. It had a mode for automatic keying based on secure distribution of the classified cryptographic key from a secure (electronic) key distribution center. NSA funded deployment of the network.[11]

A successor, the Secure Telephone Unit II (STU-II), was developed by NSA in the early 1980s for protecting classified information up to Top Secret Compartmented, depending on the classification of the cryptographic key. The STU-II program also implemented a secure key distribution center.[12] STU-II phones, which cost about $12,000 each, operate over ordinary telephone circuits and could be purchased until December 1986. The General Services Administration (GSA) was made system manager to support the purchase, operation, and maintenance of more than 3,000 STU-II phones by civilian agencies, according to NSA.[13]

The new STU-III program was announced by NSA in March 1985, subsequent to NSDD-145. STU-III units will be produced for use by Federal agencies, Government contractors, and certain other private sector firms. NSA, which will manage the cryptographic keys, plans to produce 500,000 phones at $2,000 each. As of late 1986, orders for 49,640 units (to be delivered in late 1987) had been placed, with options for additional units. The average unit price was $3,827. As of January 1987, 37,116 of the initial orders were for defense agencies and 9,675 for nondefense agencies. About 200 STU-III phones had been ordered by Government contractors.[14] The STU-III program is discussed in more detail later in this chapter.

---

[8] "Carter Approves Plan to Combat Phones by Other Nations," *New York Times*, Nov. 20, 1977, p. 34.

[9] Harold E. Daniels, NSA S-0033, Feb. 12, 1987, p. 2 of Enclosure 3.

[10] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," OTA contractor report, reference 12, November 1986.

[11] NSA S-0033, op. cit., p. 2 of Enclosure 3.

[12] In the STU-II Program, key distribution for the civil agencies is handled by GSA Key Distribution Centers. GSA is the overall Government manager for the Federal Secure Telephone System (STU-II phones), serving some 65 to 70 agencies and managing their STU-II installations, maintenance, system management, and procurement. In the successor STU-III Program, the NSA will do all keying through the NSA Key Management Center. Source: Discussion between OTA staff and GSA Special Programs Division and Electronic Services Division staff, Oct. 8, 1986. The STU-III phones will be procured commercially; plans for maintenance and servicing have not yet been announced.

Under the FSTS Systems Manager charter from NSA, GSA supports FSTS operations governmentwide, including operating the FSTS Key Distribution Centers (KDCs). It serves users in the defense and civil agencies, as well as some private consultants to the Government. Source: Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, p. 3 of Enclosure 3.

[13] NSA continues to provide a portion of the cost to sustain GSA's systems manager responsibilities.

[14] NSA S-0033-87, op. cit.

Government Procurements

GSA issued the first public competitive procurement for private line protected service between Washington, D.C. and San Francisco in 1980. This set the precedent for numerous subsequent procurements, particularly in having the carriers provide protection. A turnkey system was provided by RCA American with integrated protection for about a 5-percent cost premium over the unprotected service. The 5-year contract cost about $15 million to protect 312 circuits.

More recently, the Defense Communications Agency (DCA) awarded a major contract to AT&T for a nationwide, all-digital service called the Defense Commercial Telecommunications Network (DCTN). The 10-year, $1-billion program provides optional encrypted service among 161 locations, with link encryptors integrated into the carrier's earth stations. DCTN is designed to be flexible enough to allow for changes in technology and in customer requirements over the 10-year period. It also permits the use of video teleconferencing, switched voice, Autovon, and a wide range of data modes. DCA has also awarded a $100-million contract to Hawaii Telephone for a secure turnkey network called the OAHU Telephone System.

The largest program to date is for GSA's Federal Telecommunications Service-2000 (FTS-2000), a commercial communications service for Federal agencies.[15] FTS-2000 will eventually replace GSA's current long-distance telephone system, which has some 1.3 million subscribers who total 1.5 billion call-minutes per year.

FTS-2000 differs from the current system in that it will procure telecommunications services rather than leased facilities. FTS-2000 includes contractor-provided security features. GSA expects to award a contract by late 1987, with services to begin in 1988 at an expected first-year cost of $350 million. FTS-2000 is intended to be compatible with the evolving all-digital systems, generally referred to as the Integrated Services Digital Network (ISDN).

In its draft request for proposal, GSA required four specific security features for FTS-2000. The system has to:[16]

1. protect terrestrial radio systems in certain geographic areas and the communications links of any satellite system used to provide services;
2. provide protection from loss, degradation, or alteration by intrusion for the portion of those databases and information processing systems that are critical for continued reliable operation;
3. protect common channel signaling paths by NSA-endorsed encryption equipment or by other approved, nonencrypted forms of protection (e.g., fiber, cable); and
4. provide the capability to encrypt the command and control link of any spacecraft launched after June 17, 1990.

FTS-2000 is expected to significantly affect communications security in the private sector, according to National Security Agency officials. It is expected to stimulate the development of link encryptors, protected services, signaling channel protection, and command-and-control encryption for satellites, thereby making these features more readily available to the private sector and at lower prices.

Carrier Protection Services

Microwave radio systems began to be used to augment the existing AT&T cable infrastructure in the 1950s. By the 1960s they had become the dominant long-distance transmission medium. New companies providing communications services in the 1970s typically installed microwave circuits or used new communication satellite technology. In the 1980s, optic fiber has become the favored medium for new point-to-point circuits, while satellite is still preferred for many broadcast applications.

---

[15] Information Securities, Inc., OTA contractor report, "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," November 1986, and OTA staff discussions with GSA officials August 1986.

[16] Information Securities, Inc., OTA contractor report, "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," November 1986, reference 19.

(See ch. 3 for a discussion of the vulnerabilities of these systems.)

The protected services offered by the communications common carriers stem in large part from Government efforts in the 1970s to develop and install safeguards for microwave circuits. Satellite carriers also developed various means of encrypting transmissions relayed by their geostationary satellites. These efforts were sparked by Government encryption requirements and, in one instance, by anticipated commercial demand. Several major carriers are developing various additional services, including protected private-line services, microwave and satellite link encryption, and all-fiber networks.

At present, the interexchange carriers have announced no plans to directly protect the proposed Integrated Services Digital Network. Standards for this future network have not been decided. Nor has it been determined whether U.S. or European designs will be used. A large number of switch and PBX manufacturers are committed to providing ISDN-compatible interfaces to their customers. Users wishing to secure ISDN service can follow one of two strategies: demand protection from each carrier for the portion of the circuit provided by that carrier (link protection) or encrypt their own communications from end to end.[17] End-to-end encryption would be under the user's control, with the encryption taking place in the user's PBX, in the carrier's Centrex service, or at the ISDN interface.

DoD Programs Under NSDD-145

DoD Outreach Programs.—According to National Security Decision Directive 145 (NSDD-145), the Secretary of Defense is the executive agent for telecommunications and information systems security, with the national manager being the Director of the National Security Agency (NSA), as discussed in chapter 6. Therefore, most programs initiated under NSDD-145 are under the auspices of the National Telecommunications and Information Systems Security Committee (NTISSC), which is chaired by an assistant secretary of defense. According to NSA, the approach being taken is to focus on the national interest in addressing information security, and to develop integrated and coordinated safeguards for classified and unclassified information rather than to segregate information security concerns into defense and civilian needs. By developing integrated standards for defense and civilian agencies and for private sector use, NSA hopes to lower the cost of safeguard products and, thereby, increase their use.[18] OTA was unable to obtain an unclassified summary of all programs initiated by DoD under NSDD-145.

The following summarizes selected DoD programs under NSDD-145 that affect civil agencies and the private sector. It is based on materials provided by NTISSC.[19]

- *Civil Agency Customer Support*: A branch within the National Computer Security Center (NCSC) was organized in 1986 to provide services to civil agencies and departments, including:
  - —onsite security enhancement reviews to identify threats and vulnerabilities, and provide recommendations for improvements;
  - —technical consultations and/or one-time review visits (less detailed reviews);
  - —assistance in preparing proposals for trusted computer system procurements;
  - —assistance in drafting security policies; and
  - —briefings on computer security, NCSC, and other related topics.
- *Trusted Computer System Training*: NSA issued the *Department of Defense Trusted Computer Systems Evaluation Criteria*, also known as the "Orange Book," to all Federal agencies and departments in No-

---

[17] As of late 1986, DoD appeared to be favoring a link encryption strategy. Commercial users, who do not have control over the circuit infrastructure, may be more likely to choose end-to-end encryption.

[18] Harold E. Daniels, Jr., NSA S-0040-87, Feb. 20, 1987, Enclosure A.

[19] Letter from Donald C. Latham to OTA, NTISSC-089/86, Nov. 7, 1986.

vember 1985 for consideration as a national standard. To aid this review, NCSC presented briefings and tutorials to more than 70 Federal agencies.

- *Special Assistant for Civil and Private Sector Programs*: To fulfill its obligations under NSDD-145, NCSC, in the summer of 1986, created a senior-level position for a person to help define future directions and strategies for NCSC interactions with the civilian agencies and the private sector.
- *Computer Security Training for Civil Agencies*: NCSC has organized and is giving courses in computer security to Federal employees of the civilian agencies. The one-week courses are given twice a year and are open to all Federal agencies. Also, NCSC has initiated an annual computer security training seminar to allow computer security trainers throughout the Federal Government to exchange information on effective methods.

Data Encryption Standard (DES) Endorsement Program.—Launched by NSA in October 1982 (before NSDD-145), this program is designed to test and endorse equipment using DES to protect national security-related telecommunications in compliance with Federal Standard 1027.[20] Under the program, vendors wishing to supply endorsed cryptographic products for unclassified use by Government agencies and contractors submit their DES components (electronic devices) to the National Bureau of Standards (NBS), which validates the component's correct implementation of the DES algorithm. NSA then determines whether the product meets all other Federal requirements for endorsement and certification.

By October 1986, 32 families of equipment (17 voice, 14 data, and 1 file encryptor), totaling some 400 models, had been formally endorsed.[21] These products are available to protect unclassified Government information and all levels of sensitive private sector information.

NSA announced in 1986 that it would terminate the DES Endorsement Program in 1988 in favor of the Commercial Communications Security Endorsement Program (see below).[22] According to NSA, the change was a result of several factors, including the fact that DES has been a widely applied public algorithm for 15 years and, as such, a worthwhile target for adversaries. Therefore, NSA considers it prudent for DES to be phased out over time.[23]

The announcement has led some users to infer that DES is now unsound and, reportedly, to delay adopting safeguards because of confusion over the longevity of DES and the roles of NSA and NBS in setting standards for cryptographic algorithms.[24] In particular, the American Bankers Association, which says that the U.S. banking industry had already invested years of work and several million dollars in DES-based equipment, spent 16 months (from October 1985 to February 1987) educating NSA about their business needs. ABA spokesmen have said that, "Our industry has lost momentum in adopting improved security technology, and it remains to be seen if we can overcome the damage that has been done to the perceived security of DES-based techniques."[25]

Commercial Communications Security (COMSEC) Development Programs.—One of NSA's stated goals is to "make high-quality, low-cost cryptography available to qualified communications manufacturers for embedding in their products."[26] According to NSA, "qualified" manufacturers of such products must meet four basic criteria.[27] These are:

---

[20] "Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard," Apr. 14, 1982.

[21] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," OTA contractor report, November 1986, ref 14.

[22] According to NSA, DES products endorsed prior to Jan. 1, 1988 can be used indefinitely. Harold. E. Daniels, NSA S-0033-87, Feb. 12, 1987, p. 4 of Enclosure 3.

[23] Harold E. Daniels, NSA S-0033-87, Feb. 12, 1987, p. 4 of Enclosure 3.

[24] Peter Hager: "NSA Plan to Replace DES Draws Criticism," *Government Computer News*, May 9, 1986. Cheryl W. Helsing, Testimony on Behalf of the American Bankers Association before the House Committee on Science, Space and Technology, Feb. 26, 1987.

[25] Ibid., Cheryl W. Helsing.

1. The firm must not be under foreign ownership, control, or influence, as prescribed by the Defense Investigative Service (DIS).
2. The firm must have or obtain a DIS facility clearance because the cryptographic design information is classified even though the resultant products are not.
3. The product host in which the firm proposes to embed cryptography must, in NSA's estimation, make obvious market sense.
4. The company must demonstrate that it can produce products that meet or exceed NSA's minimum standards of quality and reliability.

NSA has established two programs to achieve its goal: one to develop the host products and the other to develop the embeddable cryptographic modules. The first, called the Commercial Communications Security Endorsement Program (CCEP), is a "business method" partnership between NSA and U.S. firms to develop a variety of secure products, such as personal computers, radios, and local area networks. The approach pairs NSA's cryptographic expertise, as embodied in embeddable modules that implement secret NSA cryptographic algorithms, with vendors' investments to develop host products that incorporate the modules. According to NSA, the industry partner then sells a "value-added" product. As of November 1986, NSA had about 40 such partnerships arranged through memoranda of understanding.[28] The first CCEP secure system was available in 1986.[29]

The second program is another joint NSA/industry venture called the Development Center for Embedded COMSEC Products (DCECP). Eleven large U.S. corporations—Harris, Motorola, RCA, Rockwell International, Hughes Aircraft, GTE, AT&T Technologies, IBM, Xerox, Intel, and Honeywell—have joined with NSA to produce modules for use in products to be developed for the commercial COMSEC program. According to NSA, these corporations were chosen based on their expertise in making selected telecommunication products. Each firm will manufacture one or more types of the NSA modules after NSA has evaluated and approved them. Each manufacturer may embed its modules within its own host equipment, a personal computer or a secure telephone, for example, and/or sell the modules to other "qualified" host equipment manufacturers. Commercial divisions in each corporation are assisting in the design and review of the standard modules to ensure that they can be used in a wide variety of commercial equipment.[30]

In addition to the list of endorsed DES products mentioned above, NSA also maintains lists of endorsed information security products and potential products. The information security products on these lists have been evaluated and endorsed by NSA as having met standards or requirements for use by the Government and its contractors to protect classified or unclassified, but sensitive information. The endorsement certifies cryptographic systems as having met NSA security specifications for a specified level of security. Items on their potential list are under development. As of December 1, 1986, 14 firms and some 30 cryptographic products were on the endorsed list; about 30 firms and products were on the potential list.

---

[26] NSA Press Release for Development Center for Embedded COMSEC Products, Jan. 10, 1986 (enclosure in letter from D. Latham to OTA, Nov. 7, 1986).

[27] Letter from Harry Daniels to OTA, Feb. 12, 1987, p. 5 of Enclosure 1. According to NSA, these criteria are prudent and not overly burdensome to potential participants. However, the requirements for security clearances from the Defense Investigative Services might be seen as burdensome by some firms, especially smaller firms that do not ordinarily need them for their personnel.

[28] "Commercial COMSEC Endorsement Program," enclosure in letter to OTA from Donald Latham, Nov. 7, 1986.

[29] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," OTA contractor report, November 1986, p. 38.

[30] Ibid., and NSA S-0033-87, p. 6 of Enclosure 3.

Further, NSA lists computer systems, software, or components that have been evaluated according to DoD's evaluation criteria for trusted computer systems. NSA also lists companies that provide communications encryption services and equipment evaluated according to the National TEMPEST Standard (NACSIM 5100A).

Standard NSA Product Line of Cryptographic Modules.—The "modules" being developed under the DCECP are sets of integrated circuits or printed wiring boards incorporating these "chip sets." According to NSA, each module is a general-purpose cryptographic device for digital data. The standard modules are designed to be transparent to the user, with a flexible, microprocessor-compatible interface and control structure.[31] The standard module approach is intended by NSA to foster development of interoperable secure systems, using well-defined interfaces and common design features throughout the family of standard modules.

In its announcement for the standard Type 1 product line intended for classified digital information, NSA noted such additional features as tamper resistance, electronic and/or over-the-air re-keying, and enhanced transmission-error detection. There are four Type 1 modules, for classified applications in three general bandwidths. There also will be three Type 2 modules, intended for unclassified, but sensitive applications.

Names, specifications, and applications of the Type 1 modules are as follows:

- *WINDSTER*: Data rate up to 200 kb/s; 9 cryptographic modes; suitable for hand-held radios, pocket pagers, and telephones. (Note: A lower performance module called INDICTOR is also available.)
- *TEPACHE*: Data rate up to 10 Mb/s; 6 cryptographic modes; suitable for minicomputers, modems, local area networks, and word processors.
- *FORESEE*: Data rate up to 20 Mb/s; 7 cryptographic modes; suitable for satellite links, microwave links, fiber optic links, and mainframe computers.

Type 2 modules, which will be available at an unspecified future date, have been given the names EDGE SHOT (same data rate as WINDSTER), BULLETPROOF (same data rate as TEPACHE), and BRUSHSTROKE (same data rate as FORESEE). Types 1 and 2 modules are intended to be interoperable within each bandwidth.[32] NSA plans to key Type 1 modules through a secure key management system. It is not clear whether private firms that choose to use Type 2 modules will be able to control key generation independently of NSA.

NSA notes that the modules are designed to perform more system security functions than if they contained just a "naked" key generator chip and to leave fewer security functions for the host vendor to add on. However, to accommodate a wider range of commercial host products, NSA has an alternative commercial Type 2 "naked" key generator chip available to potential host vendors. Type 2 modules will be made available to qualified firms that have a memorandum of understanding with NSA, to firms under contract with NSA or other Government agencies to develop a crytographic product, to Government agencies doing cryptographic development, and to certain other firms approved on a case-by-case basis.[33]

Some users have expressed concerns that the embedded cryptography will not be readily compatible with their existing equipment and operations, and others note that the change is damaging to manufacturers of DES equipment. To ease the transition, NSA had offered to work with manufacturers of the Data Encryption Standard (DES) components and develop pin-for-pin replaceable circuits using the new NSA algorithms, so that equipment manufacturers' investments in product designs would not be lost. According to NSA, none of the DES component manufacturers expressed interest in this plan.[34]

---

[31] "Off the Shelf Information Security Products: A Family of User-Friendly Modules for Embedding Within a Wide Range of Telecommunication Systems," NSA; enclosure to letter from D. Latham to OTA, Nov. 7, 1986.

[32] Information on Types 1 and Type 2 modules were provided by NSA at a meeting of the IEEE Subcommittee on Privacy, June 18, 1986.

[33] Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, pp. 8-9 of Enclosure 3.

STU-III Program.—NSA initiated the Secure Telephone Unit III (STU-III) program in 1984 to develop a new generation of secure telephone equipment using classified NSA algorithms (but not the standard modules being developed under the DCECP program). NSA intends that the STU-III program serve all Government agencies and private companies that require telephone security. NSA-sponsored studies have estimated a market for 2 million units, with DoD being the largest single buyer. Market studies by vendors also indicate potential sales of 1 million to 2 million units to the private sector,[35] although these conclusions are admitted to be soft. According to NSA, the STU-III program will feature the capability for multilevel security, availability of Type 2 units to the private sector, and interoperability among all STU-III users. This will make the units attractive to a broad range of Government and private sector users.

The first production contracts were awarded in July 1986 to three vendors—AT&T, RCA, and Motorola. They are authorized to market their Type 2 product directory to the private sector. The 2-year, fixed-price contracts totaled about $190 million for 49,640 units. (See section above on Secure Voice Programs.)

NSA reports that the STU-III vendors still consider the government-contractor and other segments of the private sector market to be "embryonic," in that customers have expressed interest but are waiting to see the product. Sample Type 2 units will be available in 1987, at which time vendors are expected to begin more active marketing efforts. According to NSA, Type 2 units could be delivered to private sector customers beginning in January 1988. The production contracts contain an add-on option allowing additional STU-IIIs (see above) to be produced at a reduced unit cost, in the $2,400 to $2,600 range.[36]

Almost all of the current order was for Type 1 units intended for classified uses, but 300 Type 2 units for unclassified, but sensitive information were also included in the initial contract. NSA will be the source of all cryptographic keys for the STU-III phones, including those purchased by private sector users. For the Type 2 phones, users will be able to establish their own internal procedures for key management, except key generation. Type 2 users within the Government will obtain their keys directly from NSA; private sector users will order keys from NSA via their STU-III vendors.[37]

The Secure Data Network System.—The Secure Data Network System (SDNS) project seeks to design an architecture for secure computer networks. The project will provide a security architecture design for networks that transmit digital data between computers. The project, certain aspects of which are currently classified, is sponsored by NSA and includes participation by NBS, the Defense Communications Agency, and about a dozen computer and communications vendors.

SDNS is intended to support both classified and unclassified applications. The system will provide confidentiality, data integrity, message authentication, and access control services. The services and standards for them are being designed to be compatible with those being developed by the International Organization for Standardization (ISO). Currently, the project is in the prototype development stage. Hardware is being developed and tested for performance, interoperability, and conformance with ISO standards.

---

[34] Harold E. Daniels, NSA S-0033-87, Feb. 12, 1987, p. 4 of Enclosure 3.

[35] "STU-III Program Status," enclosure in letter from D. Latham to OTA, Nov. 7, 1986.

[36] NSA response to OTA questions on STU-III: NSA S-0033-87, Enclosure 1, Feb. 12, 1987.

[37] Ibid.

Encryption capabilities will be provided with two different NSA-supplied algorithms, both of which will remain classified. A Type 1 algorithm will be used for encrypting classified information and a Type 2 will be used for unclassified but sensitive information.

Raising Private Sector Awareness.—The Federal Communications Commission (FCC) is taking steps to alert the private sector to the vulnerabilities of communications systems. The FCC recently issued for NSA a public notice advising licensees and users that "the Nation's telecommunications systems, particularly those involving terrestrial microwave transmission media and satellites, are extremely vulnerable to unauthorized access."[38] This notice, which also applies to telecommunications services or equipment that bypass public-switched services, encourages concerned users to seek assistance from NSA in "identifying approved devices for the protection of sensitive, but unclassified, national security-related communications (Government or nongovernment)."[39]

Implications of Merging Defense, Civilian Agency, and Private Sector Requirements

Advocates of combining security standards for unclassified information and guidelines for Government agencies with those for the private sector argue that aggregating markets will permit manufacturers to enjoy production economies and result in lower prices for safeguard products. Moreover, some feel that the current markets for computer and communications safeguards, particularly for trusted operating systems and cryptographic products, are "fragile." They argue that one coordinated set of Federal standards is needed to encourage and strengthen these markets. Critics of the present approach of National Security Agency (NSA) standards development and product certification see these as not fully responsive to current and evolving defense, civilian, and business needs.

There is some early evidence that NSA has already begun to encounter difficulty in satisfying the diverse needs of the private sector, beginning with the banking industry. (See ch. 6.) Moreover, NSA's controlling role may raise barriers to market entry by new vendors. At a more fundamental level, NSA's national security and signals intelligence interests in controlling encryption technology appear in tension with its new role in developing and disseminating safeguard technologies and products. (See below and ch. 7.)

Possible Barriers to Market Entry.—Only "qualified" manufacturers meeting the NSA criteria noted earlier will have access to NSA designed and endorsed standard cryptographic modules. Moreover, there will be accountability requirements for all modules and, even though the hardware modules themselves will be both unclassified and tamperproof to prevent reverse engineering, NSA may place restrictions on their export. (See below.)

The embeddable modules are being produced by the 11 large electronics firms mentioned above, NSA's "industry partners." Because of the limited number of these firms and because they will most likely also produce host products incorporating the modules (for the Commercial Communications Security Endorsement program), some prospective entrants into the host product market have expressed concern that competition in this potentially lucrative market will be essentially limited to firms already participating in the module program. Faced with the prospect of purchasing the embeddable modules from large, vertically integrated competitors, some prospective entrants fear that NSA's tight controls on its commercial programs will limit competition.

NSA, on the other hand, does not consider the qualification criteria particularly burdensome, but, rather, reasonable. For instance, NSA notes that there are over 13,000 Defense Investigative Service cleared facilities in the United States and that cryptographic design information is classified with access limited to U.S. entities in accordance with prudent overall security considerations. Similarly, NSA considers that decisions about the quality and market criteria will be fairly executed, with ample opportunity for vendors and potential vendors to present their cases. According to NSA, host vendor participation in the CCEP program has already exceeded participation in the DES Endorsement Program.[40]

---

[38] Federal Communications Commission, Security and Privacy of Telecommunications, Public Notice 6970, Sept. 17, 1986.

[39] FCC Public Notice 6970, Sept. 17, 1986.

As to competition in the host product market, NSA's stated intent is to make the Development Center for Embedded Communications Security Products (DCECP) modules competitively available to host manufacturers. All 11 of the DCECP module vendors have access to both Types 1 and 2 design documentation and, according to NSA, it is a vendor decision as to which module(s) to fabricate and produce. The Government owns the designs and NSA has stated that, should a particular module not be chosen by any of the 11 manufacturers for fabrication and production, or should there not be competitive sources for a given module, then the agency will seek additional sources for the modules. NSA also notes that, in order to achieve scale economies, competitors may sell to each other—a practice that is common in the electronics industry.[41]

DoD Control of Encryption Technology.—NSA sees its signals intelligence mission to be at risk if effective cryptography were available worldwide. As a result, NSA faces tensions between its missions of encouraging domestic use of effective encryption and other safeguards while controlling the transfer of encryption technology overseas. Thus, its strategies to improve the availability of safeguards for use by U.S. nondefense Government agencies and businesses also include controls on the dissemination of such products and technical data, some of which have already begun to cause new tensions with the private sector.

Cryptographic hardware and software are controlled by bilateral agreements and by patent and export control legislation and regulations, including the Export Administration Regulations, the Invention Secrecy Act (35 U.S.C. 181 et. seq.), and the International Traffic in Arms Regulations (ITAR),[42] as discussed in chapter 6. All equipment and systems based on DES, including those for automatic data processing file security and message authentication for electronic fund transfers, are included on the ITAR Munitions List and fall under the jurisdiction of the Department of State's Office of Munitions Control (OMC). OMC licensing agreements are coordinated with NSA.[43]

The exportability of cryptographic safeguards is an important consideration for many businesses that have overseas correspondents or subsidiaries. Prominent among these is the banking industry, which has spent some years developing techniques and standards for transaction authentication and confidentiality. These are based on DES, which can be licensed for export and use abroad. When NSA announced its planned replacement of DES with secret (CCEP) algorithms, bankers and the American Bankers Association (ABA) became concerned that the CCEP algorithms and modules could not be used by the financial industry as a substitute for DES. For one thing, reliance on one or a few algorithms would be unacceptable for use in some foreign countries or banks, even if NSA would permit their use abroad. Also, according to the initial NSA announcement, the (Type 2) modules may not be used internationally or placed in equipment for use by non-U.S. entities.

Finally, the bankers found the prospect of NSA retaining control of the cryptographic keys to be an unacceptable transfer of bank responsibility to a Government agency. As of mid-1987, NSA and ABA were still discussing whether NSA would provide an acceptable exportable module for use overseas to authenticate financial transactions. In mid-February 1987, NSA and ABA reached agreement that NSA would continue to support the financial industry's use of DES-based technology until an acceptable replacement is available.[44]

---

[40] Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, pp. 8-9 of Enclosure 2; p. 5 of Enclosure 3.

[41] Ibid., pp. 8-10 of Enclosure 2.

[42] Multilaterally agreed upon export controls are determined through an international coordinating committee (COCOM) whose membership includes representatives of the United States and 13 U.S. allies.

[43] J. Smaldone, Office of Munitions Control, personal communication with OTA staff, Sept. 24, 1986.

NSA appears to be reconsidering the exportability issue for Type 2 modules. In February 1987, in response to a question from OTA, NSA officials stated that:

> The NSA desires that host products employing Type 2 modules be usable by U.S. entities outside the U.S. For example, a U.S. firm operating in Europe should be able to purchase and use a Type 2 product, or a foreign subsidiary should be able to use a Type 2 product as long as ownership was maintained by a U.S. entity. Use by foreign firms or individuals, when it is in the U.S. interests for interoperability is possible, depending on the country involved and inter-country agreements.[45]

The various NSA outreach and industry partnership activities seem tailored to the agency's dual missions of encouraging the use of safeguards while controlling the spread of cryptographic and cryptanalytic expertise. For the former, NSA uses site visits, briefings, exchanges of personnel and information, and product evaluation and endorsement in addition to written standards and guidelines. For the latter, NSA makes cryptographic hardware and interface specifications generally available to host equipment vendors and users, without broadly transferring expertise in cryptographic design and cryptanalysis. For instance, it is unclear whether even the 11 module manufacturers know all the cryptologic criteria used by NSA in developing the algorithms, although NSA gives them the design information and expertise needed to manufacture the hardware that implements the algorithms.

In contrast, the DES standard as promulgated is public information, not limited to specific manufacturers and vendors, and provides more visibility into the algorithm itself. The fact that the algorithm was published made possible independent evaluations of its robustness, as well as (unvalidated) software implementations, thereby contributing to private sector capabilities in commercially useful cryptography.

On the other hand, NSA believes that assertions to the effect that current policies and the DCECP and CCEP programs limit competition and stifle private sector innovations and development are unsupported. According to NSA officials, the agency is actively encouraging private sector innovation and the development of information safeguards for business needs. For example, NSA cites the CCEP program, in which prospective host product vendors determine which products to produce based on their assessments of market needs.

Moreover, part of the rationale for NSA's approach is to use interfirm competition to drive down the cost of information security products like the STU-III phones. NSA and the rest of DoD have been concerned that relatively high costs have limited their use within DoD and elsewhere. The resulting small market was not attractive to producers. By making information security products more affordable, NSA hopes to increase their availability and use. In achieving this, according to NSA, "technological competitiveness is the goal in driving costs down versus cryptographic competitiveness which does nothing for cost and can have a deleterious effect on national security."[46]

Technology Development and Dissemination.—After a number of DoD-sponsored studies and demonstration projects during the 1970s to address technical problems associated with controlling the flow of classified and other information in multiuser computer systems, the DoD Computer Security Initiative was started in 1977. Concurrently, the National Bureau of Standards (NBS) began to define the construction, evaluation, and auditing of secure computer systems. As an outgrowth of recommendations from a 1978 NBS workshop paper on criteria for evaluating technical computer security effectiveness, and in support of the DoD Computer Security Initiative, the MITRE Corp. began to develop a set of criteria for assessing the level of trust that could be placed in a computer system to protect classified data.

---

[44] Cheryl W. Helsing, Testimony on Behalf of the American Banking Association before the House Committee on Science, Space, and Technology, Feb. 26, 1987.

[45] Op. cit., Harold E. Daniels, Jr., NSA S-0033-87, p. 10 of Enclosure 2.

[46] Harold E. Daniels, Jr., NSA S-0040-87, Feb. 20, 1987, Enclosures D and E.

In 1981, the DoD Computer Security Evaluation Center was established to continue the work started under the DoD Computer Security Initiative. The center, located within NSA, was renamed the National Computer Security Center after its responsibilities were expanded by National Security Decision Directive 145 (NSDD-145).

The National Computer Security Center (NCSC) developed the "Orange Book" criteria for evaluating multilevel security in commercial computer systems. The original criteria were published as the Department of Defense Trusted Computer System Evaluation Criteria (CSC-STD-001-83, August 15, 1983). A derivative but slightly different document was later published as DoD 5200.28-STD in December 1985. The Orange Book criteria evolved from the earlier NBS and MITRE work.[47] NCSC has also released "Yellow Books" that help users apply the comprehensive Orange Book criteria to specific computer facilities.[48]

The criteria specify four divisions, ranging from Division D (minimal protection) up through Divisions C (discretionary protection) and B (mandatory protection), to the most comprehensive Division A (verified protection). Each division represents an improvement in the overall confidence that can be placed in the system to protect information. Within divisions C and B, security classes such as C1, C2 or B1, B2, and B3 correspond to progressively stronger security features.

NSA produces a number of computer security documents ranging from trusted operating systems (the "Orange" and "Yellow Books") to forthcoming criteria for trusted computer networks and data bases.[49] Some users apparently have reported difficulties in interpreting the Orange Book criteria at the higher protection levels; as one response to this, NSA has developed a rules-based expert system available to guide users through the Yellow Books.

The Orange Book criteria have been adopted as a DoD standard (DoD 5200.28-STD, December 1985), and therefore these security requirements must be included in specifications for new systems being developed by DoD. However, the question of whether the Orange Book criteria and evaluated products program will best serve the unclassified, but sensitive information security needs of civil agencies and the private sector is being debated within the computer-security community, especially outside NSA. (See the section below on differences between military and commercial models of security.) As of May 1987, the NCSC's Evaluated Products List reported security class ratings according to the Orange Book criteria for 8 products, and about 20 more products were being evaluated.[50]

---

[47] From information on the history of the Orange Book criteria contained in DoD 5200.28-STD, which provides a more detailed history and rationale for the trusted computer system evaluation criteria.

[48] DoD Computer Security Center: "Computer Security Requirements: Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments (CSC-STD-003-85)," June 25, 1985; and "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements (CSC-STD-004-85)," June 25, 1985.

[49] Presentation by P. Gallagher of NSA, at an IEEE Subcommittee on Privacy meeting at George Washington University in Washington, D.C., Nov. 13, 1986.

[50] Some information on the evaluated products program was contained in a letter from Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, p. 7 of Enclosure 2. See also: National Computer Security Center, *Evaluated Products List for Trusted Computer Systems*, Dec. 1, 1986 (updated May 31, 1987).

OBJECTIVES AND PROGRAMS UNRELATED TO NATIONAL SECURITY

Background

As part of this study, OTA surveyed the data and information security procedures, policies, and practices of large U.S. corporations. The survey also tried to determine the extent to which these firms are aware of Government-sponsored assistance and whether they have been affected by National Security Decision Directive 145.

The survey was self-administered at an October 1986 meeting of Palmer Associates, a group of computer audit directors of Fortune 100 companies. Questionnaires were completed by all 26 people present, a sample that is far too small to be representative of U.S. industry at large or for statistical generalizations.

Nevertheless, the results are of value for two major reasons. First, they illustrate the perceptions of some knowledgeable corporate leaders about security needs and practices. Second, the vast majority of the respondents were from nondefense companies (92 percent, with 42 percent from banking alone), while most of NSA's experience with the private sector has been with defense contractors. The survey results may shed some welcome light on the desirability and feasibility of NSA's plans to meet aggregated users' needs with one set of standards, guidelines, and technologies, and can provide a context for the section below on differences between military and commercial models of information security.

Also, the consulting firm of Ernst & Whinney included some of the same questions in a separate survey that was self-administered by attendees of the Computer Security Institute's 13th Annual Conference held in November 1986 in Atlanta, Georgia. A total of 562 completed questionnaires (a 12 percent response rate) were returned on site or by mail; 141 responses (25 percent) were from Government employees and the remainder came from a broad spectrum of business and industry. Of the respondents, another 18 percent were from manufacturing, 15 percent from financial services, 9 percent from insurance, and 8 percent from communications firms. Only 3 percent of the respondents identified themselves as from the defense industry. With Ernst & Whinney's permission, some of their survey data are used in this chapter, in addition to the OTA survey data.

Private Sector Motivations

Private industry and civilian agencies want information safeguards to:

- protect corporate proprietary or sensitive information from unauthorized disclosure or access and ensure the integrity of data and its processing;
- reduce losses from fraud and errors in electronic funds transfers and other financial transactions, limit associated increases in insurance premiums, and limit exposure to legal liabilities for preventable losses; and
- take advantage of new opportunities to reduce costs.

Box E provides several indicators of increased private sector interest in electronic safeguards.

Protection of valuable corporate electronic information from disclosure (confidentiality) is important to many firms, but this need is not necessarily a firm's major concern for information security. The OTA survey found that the 26 respondents placed roughly equal importance on integrity, confidentiality, and

Box E.—Indicators of Private Sector Interest in Safeguards

Even though many industry spokesmen consider the market for many advanced safeguards fragile and emerging, OTA has noted a number of indications of growing private sector interest in improved safeguards, including:

- *Rapid growth in the number of computer-communications security conferences during recent years and in their attendance levels.*—Attendance at the National Computer Security Conference, sponsored jointly by the National Security Agency (NSA) and the National Bureau of Standards (NBS), increased three-fold in the last 7 years, from about 350 in 1980 to more than 1,000 in 1986. Capacity constraints at NBS conference locations have forced sponsors to limit attendance. Some other conferences, such as the Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy are also limited by space constraints. Attendance at the Computer Security Institute's annual Computer Security Conference/Exhibition doubled—from 600 to 1,200—between 1981 and 1985, and the American Society for Industrial Security Seminar and Exhibition has expanded to include computer security, biometrics, and access control. In addition, many new conferences and workshops given by security consultants and user groups have sprung up over the past 3 years. Among the latter are conferences and workshops for users of the Top Secret and RACF access control software packages. Other annual conferences include CRYPTO in the United States and EUROCRYPT, both sponsored by the International Association of Cryptologic Research.
- *Increases in the level of sales of safeguard equipment and software.*—According to market reports, installations of two of the most popular commercial access control software packages, ACF2 and Top Secret, have grown by more than a factor of 10 over the past 6 or so years.
- *The rise in the number of computer and communications security consultants and in the number of organizations for security professionals.*—The number of security consultants listed in directories have increased, and new professional groups are forming, such as the Information Systems Security Association (ISSA). Consulting firms are expanding their information security practices and new services organizations are being established. such as the International Information Integrity Institute (SRI International).
- *The increasing number of technical articles being published on topics related to computer and communications security.*—OTA staff did a word search using the abstracts of articles published in the ABI/INFORM journal set, a collection of more than 650 U.S. and foreign business publications including such areas as accounting, banking, data processing, economics, finance, insurance, and telecommunications. The 200-word abstracts for the years 1971, 1976, 1981, and 1985 were searched for 5 selected phrases (computer security, communications security, encryption, data integrity, and personal identification) in order to determine whether the relative frequencies of these had increased. OTA found that the number of abstracts including these phrases had grown in real as well as nominal terms, in particular, the phrase "computer security" occurred in only one out of 1,737 abstracts in 1971, but occurred in 268 out of 38,375 in 1985—a 10-fold increase in relative frequency (none of the other 4 phrases occurred in any of the 1,737 abstracts in 1971). The phrases "data integrity" and "encryption" occurred in only two and eight out of 14,356 abstracts, respectively, in 1976. By 1985, they occurred in 45 and 85 out of 38,375 abstracts, respectively—a three-fold and ten-fold increase in relative frequency. The phrases "personal identification" and "communications security" occurred infrequently and did not show significant increases in relative frequency.

reliability/continuity of service as components of their organization's information security, with integrity being rated slightly more important overall. The larger Ernst & Whinney survey found similar results, with both Government and nongovernment respondents rating integrity slightly higher than confidentiality and reliability/continuity. Interestingly, Government respondents rated confidentiality slightly higher than continuity of service, while the opposite was the case for nongovernment respondents.

Encryption or access control technologies can protect valuable proprietary information from disclosure, but they can also preserve its integrity and protect it from accidental or malicious modifications or deletions. This can be particularly important where large databases are a major revenue-producing asset. The regional Bell operating companies, for example, safeguard their on-line database for their *Yellow Pages* to preserve the integrity of the data and to prevent unauthorized use, not to prevent disclosure. In that sense, a recent news story reported that a disgruntled employee had attempted to rewrite parts of the 1988 edition of the *Encyclopedia Britannica*. The sabotage attempt failed, according to a company spokesman, because of safeguards that prevented unauthorized changes to the computer database.[51]

Most of the OTA survey respondents and almost 90 percent of the Ernst & Whinney survey respondents judged information security as being of "fair" or "extreme" importance to their organizations. Of the Ernst & Whinney respondents, Government respondents assigned slightly more importance overall to information security than did the nongovernment respondents.

All the OTA survey respondents noted an increase in the importance of data and information security to their firms over the past 2 years. About one-third reported "significant information or data security problems" during the past 2 years, mostly in the form of unauthorized access and loss of integrity (in one case, engineering data was destroyed). In only one instance was loss of confidentiality cited, resulting in invalid competitive bids—which may be an indication of the difficulty of detecting some misuses, rather than their absence. Only 2 percent of the information handled by these firms is classified for reasons of national security, according to respondents to the OTA survey.

The majority of Ernst & Whinney survey respondents considered that the security risks faced by their organizations have increased over the past 5 years, and about one-third of the business and one-fourth of the government respondents considered that these risks were not adequately met. Half of the respondents reported financial losses as a result of security problems or downtime, mostly under $50,000, although a few losses were reported to be in excess of $1 million (note that this question included losses due to downtime, which the OTA survey did not include). About one-third of the respondents reported non-financial losses, mostly in the form of unauthorized access by employees and hackers. For Government respondents, about 31 percent of the information mix handled by their organizations was classified for purposes of national security, versus only 4 percent for nongovernment respondents.

Reducing EFT Fraud and Other Losses.—U.S. banks transferred some $167 trillion in 60 million separate transactions in 1984. The actual amount of wire transfer fraud experienced by banks is unknown. One estimate by the Bureau of Justice Statistics suggests aggregated electronic fund transfers (EFT) and automated teller machine (ATM) losses of $70 million to $100 million a year during the early 1980s, but a large fraction of this figure is due to ATM losses from fraud (by "con men," etc.) against the owners of the bank cards. Another Bureau of Justice Statistics report examined some 139 problem wire transfers. It found an average potential loss per transaction of $800,000, although some potential losses were significantly larger.[52]

---

[51] "Britannica Sabotage Thwarted," *Washington Post*, Sept. 6, 1986, p. D3.

Similarly, an American Bar Association (ABA) survey of private and public sector organizations found that one-quarter (72) of those responding reported "known and verifiable losses due to computer crime in the last 12 months." Losses reported by respondents overall ranged from a few thousand dollars to more than $100 million. Most losses reported by the (anonymous) respondents were less than $100,000.[53]

A large survey by the American Institute of Certified Public Accountants revealed that 2 percent (105) and 3 percent (40), respectively, of the banks and insurance companies surveyed had experienced at least 1 case of fraud related to electronic data processing (EDP). Most perpetrators were employees. More than 80 percent of the frauds involved amounts under $100,000.[54]

The Department of Justice Bureau of Justice Statistics (BJS) recently examined the scope of EFT fraud, based on extrapolations from a limited sample of 16 banks. The BJS study suggested annual losses nationwide in the $70-$100 million range for automatic teller machine fraud. Twelve of the banks reported 139 wire transfer fraud incidents within the preceding five years, with an average exposure to loss (before recovery efforts) of some $880,000 per loss and an average net loss (after recovery efforts) of about $19,000 per incident.[55]

Whatever the actual amount of the losses, there is another indirect indicator that this is a serious problem: insurance premiums are rising for protection against fraud and other types of losses related to electronic transfers of funds.[56] During the past year, financial institutions' motivations to safeguard value-bearing transactions—EFTs, letters of credit, and securities transfers—have been strengthened by actions of their insurers, some of which are raising premiums and/or requiring the use of message authentication methods approved by the American National Standards Institute (ANSI). As industry applies safeguards more widely and as the use of certified safeguards becomes more commonplace, expectations for responsible corporate behavior will be raised. A new standard, and perhaps a legal criterion, appears to be evolving for gauging responsible corporate behavior, or "due care," in businesses where firms are expected to provide reasonable safeguards for information whose loss could do significant harm.

The wholesale banking industry is leading this trend, prompted by liability and "due care" considerations, by the recommendations of internal and external auditors, and by Treasury Department policies. Treasury has issued policy directives requiring all Federal electronic fund transactions to be authenticated by June 1988. Dated August 16, 1984, TD-81.80

---

[52] See U.S. Congress, Office of Technology Assessment, "Ch. 5, Computer Crime," *Federal Government Information Technology: Management, Security, and Oversight*, OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986), for an overview of the scope of computer-related crime and losses from electronic fund transfers and automated data processing.

[53] Report on Computer Crime, Task Force on Computer Crime, Section on Criminal Justice, ABA, 1984.

[54] American Institute of Certified Public Accountants, EDP Fraud Review Task Force, *Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries*, 1984.

[55] Bureau of Justice Statistics Report NCJ-100461, *Electronic Fund Transfer Systems Fraud*, April 1986.

[56] The experience of a west coast bank illustrates the magnitude of the changes in coverage being offered by insurers for EFT loss claims. Until recently, the bank's insurance coverage cost about $1 million annually, and provided protection of up to $50 million per electronic transfer claim, with a $1 million deductible. The policy premium in mid-1986 rose to $5 million, with a $10 million deductible, and an upper limit of $100 million for total annual claims. [Source: OTA staff discussion with bank officials, May 1986.]

specified that Federal EFT transactions be authenticated using measures based on DES and conforming to ANSI standards. This action is expected to have widespread effects throughout the banking industry because of the large number of systems and communications links that will use the system, and because some standards set by Treasury and the Federal Reserve System (which serves as the interface between Treasury and the wholesale banks) become defacto industry standards. As certified hardware for authentication becomes more widely used, economies of scale will lower prices for authentication hardware. As prices fall, additional end users are likely to adopt techniques and hardware to safeguard other business functions, creating a ripple effect throughout the private sector.

Thus, an early and important exception to the non-recertification of DES was made by NSA in the area of electronic fund transfers. Through a memorandum of understanding, the Treasury Department will certify commercial data security devices for securing fund transfers, with technical guidance and support from NSA and NBS. DES will remain the encryption algorithm for EFT transactions while authentication measures will be specified by ANSI standards adopted by the wholesale banking community.[57] More recently, NSA agreed to support use of the DES for bank message authentication until an acceptable replacement became available. Widespread use of DES to authenticate electronic fund transfers will increase demand for DES-based hardware. That could lower its price and encourage its adoption for other applications in wholesale and retail banking and elsewhere. As an example of a retail banking application, the DES is used to encrypt customers' personal identification numbers in interbank automatic teller machine networks in the United States and Canada.[58]

A superceding Treasury Directive, TD-16.02 (dated October 2, 1986), extended the authentication requirement to securities transfers and stated that equipment designed and used to authenticate Federal EFTs must comply with Federal Standard 1027, which specifies security requirements to be satisfied in implementing DES (FIPS Pub. 46). Keying material used in DES authentication must be generated and processed in accordance with ANSI Standard X9.9. The broader requirement is expected to speed the dissemination of authentication techniques throughout the private sector.

A number of private financial institutions are taking aggressive steps to prevent certain types of misuse. Citibank, for instance, now has more than 4,000 encrypted links overseas. Similarly, the private Clearing House Interbank Payments System (CHIPS), whose $240 billion in daily settlements is second in size only to the Federal Reserve System, uses ANSI-approved standards to authenticate its transactions.[59] Large U.S. banks have also been among the most active participants in the development of technical standards through ANSI (see below).

Reducing Costs.--Companies can also reduce the costs of routine business transactions by conducting them via computer-to-computer communications that make use of cryptographic-based authentication techniques. These inter-organization transactions use standardized formats for the electronic interchange of business data between independently organized, owned, and/or operated computer and communication systems. This is accomplished by each corporate participant assembling its transaction data in predefined sequences, called "transaction sets."

---

[57] Memorandum of Understanding #S52-99-84-018, Parts IV and V. This memorandum may be renewed in 1987, according to NBS staff.

[58] Eddie Zeitler, Security Pacific National Bank and Nancy Floyd, Citicorp/Quadstar. Personal communications with OTA staff, Feb. 18, 1987.

[59] Authentication in CHIPS, New York Clearing House, Jan. 17, 1985.

In 1986, CHIPS transactions amounted to $125 trillion, compared with $124.4 trillion in domestic transactions handled by the FEDWIRE system. The FEDWIRE system handles a greater volume of transactions than CHIPS, and has many more on-line correspondents (7000 depository institutions compared to the 121 CHIPS member banks). [Source: Florence Young, Division of Federal Bank Operations, Federal Reserve System. Personal communication with OTA staff, Feb. 13, 1987.]

Several industry-specific interchange standards have previously been developed, including transaction sets for air, motor, ocean, and rail transportation, as well as for public warehousing, and for the grocery industry. Development of an American National Standard for electronic data interchange is under way, intended to replace the many paper and special-purpose business methods by 1988. One of the long-term goals of this standard is the realization of paperless trade transactions and transportation arrangements. Standards for this purpose are being developed by the ANSI X12 Committee, which was chartered in 1978. The first set of X12 standards for electronic business data interchange was approved by ANSI in 1983, and more were published in 1986.

The national standards are intended to be broad enough to encompass all forms of business transactions amenable to standardization, including inter-industry transactions. The electronic transactions, referred to as Electronic Data Interchange (EDI) or Electronic Business Data Interchange (EBDI), are intended to reduce business costs by speeding up the purchase order cycle, reducing the inventory buffers firms must carry, and streamlining cash flow. Dozens of common transactions will be integrated using these standards, including purchase orders, invoices, shipping notices, check payment vouchers, requests for quotations, and marketing information.[60] These transactions amount to billions of dollars annually. An estimated $38 million worth of them were handled electronically in 1985; by 1990, electronic business transactions are expected to amount to more than $1 billion.[61]

These standards, or some compatible form of them, may also be adopted worldwide, thereby facilitating international transactions in different currencies. For this reason, any message authentication product, such as that required for business data interchange will have to be eligible for use in other countries. The current ANSI authentication standard, based on the DES, is exportable, but its replacement may not be.

The original focus area for electronic data interchange was in transportation, beginning in 1968.[62] The Transportation Data Coordinating Committee (TDCC) worked with representatives of the rail, motor, ocean, and air transport industries to develop EDI transaction sets for these modes. The first successful data interchange transmission occurred with railway bills, in 1975. Around the same time, TDCC organized a group of computer and communications experts to develop specific business applications of this type of electronic transaction. Among the outcomes of this group activity were the development of purchase order and invoice transaction sets and movement toward generic transaction sets for industry. In the early 1970s, large corporations, such as Sears, JC Penney, and K-Mart had started transmitting purchase orders electronically, with specialized formats. This was feasible in part because these retailers were often their suppliers' sole or largest customer. However, benefits due to improved transaction accuracy and timeliness accrued to both parties, increasing interest in electronic transactions.

Movement toward further development of generic transaction sets was formalized in 1978, when the ANSI X12 Committee was formed. TDCC and the Credit Research Foundation provided technical support to the new committee, and TDCC is the current X12 Secretariat. In 1979, the grocery industry began its industry-specific Uniform Communication Standard (UCS), which is compatible with the EDI architecture developed by TDCC for the transportation standards. Subsequently, standards for public warehousing applications (Warehouse Information Network Standards, or WINS) were developed, also compatible with the EDI architecture. These standards include various security features.

---

[60] See: Jack Shaw, "Electronic Business Data Interchange: A New Strategy for Transacting Business," *MSA Update*, Management Science America, Inc., March/April 1985; "Detroit Tries to Level a Mountain of Paperwork." *Business Week*, Aug. 26, 1985, pp. 94-96.

[61] Management Information Systems Week, Jan. 20, 1986. Estimates provided by Jack Shaw at the ANSI ASC X12 meeting on June 9, 1986 are over $3 billion by 1990.

[62] Information on the evolution of electronic data interchange standards was provided by Paul Lemme, Transportation Data Coordinating Committee, ANSI X12 Secretariat. Personal communication with OTA staff, December 1987.

The ANSI X12 Committee is developing generic standards for electronic business data interchange. In November 1986, industry representatives agreed on a common data dictionary for the ANSI X12 standards, the WINS and UCS standards, and the TDCC EDI standard.[63] The ANSI X12 Security Structures Taskgroup is developing transaction security standards under the auspices of the X12 Finance Project Team, and the X12 Committee has joined with the ANSI X9 Committee to deal with encryption and encryption-related business requirements. According to the X12 Secretariat, the latter include: electronic signatures ("telex signature"); data integrity, "hash controls" (digests); message authentication and sender verification; confidentiality of business data; error detection; end-to-end security; and protection against replay, spoofing, modification, or impersonation.

Benefits from electronic transactions are expected to be substantial for diverse user groups, and some are already being realized. In 1980, a report prepared for the American Grocery Industry projected $300 million in profits for the industry as a result of implementing standardized electronic transactions. The grocers' UCS standards were completed in 1981, and the resulting industry gains have reportedly exceeded the projections.[64] The Automotive Industry Action Group, composed of the the major U.S. automobile manufacturers and about 300 of their largest suppliers, began their movement toward standardization of electronic business transactions in 1981. According to some estimates, General Motors and Ford expect to realize a $200-per-car savings, or some $1 billion a year, on a typical production volume of 5 million cars per year, through use of electronic business data interchange.[65] Caterpillar Tractor Co. has instituted an electronic transaction system linking some 400 sites.[66]

Because of the automobile industry's large number of suppliers, contractors, and distributors, their use of the new data interchange standards is expected to accelerate the spread of these standards to other industries. These include metals, plastics, and rubber, as well as chemicals, transportation, electronics, aerospace, banking, and retail sales.[67] The movement toward electronic business transactions is giving rise to new, network-based "electronic clearinghouses" with market entrants such as IBM, GTE Telenet, GEISCO, Tymshare, and GM's Electronic Data Systems.[68]

Potential savings to the Federal Government from electronic purchasing alone have been estimated to be $20 billion/year or more.[69] The DoD, for instance, has begun to use electronic data interchange to reduce the time required to get supplies to overseas commissaries, and expects to shorten immediately the 75-day purchase cycle by 5 or 6 days, thereby reducing inventory requirements. Other commissary and procurement paperwork-reduction projects have been under way within DoD for a few years.[70]

---

[63] Elisabeth Horwitt, "Move to EDI Gathers Steam as Standards Clear, Benefits Grow," *ComputerWorld*, Dec. 15, 1986, p. 5.

[64] Paul Lemme, TDCC. Personal communication with OTA staff, December 1986.

[65] Ford's estimate is from "GEISCO Plans To Move Rockville Jobs in Bid to Get Edge in Global Markets," *Washington Post*, Sept. 29, 1986, Business Section, p. 4. The cost savings for GM is from a presentation by Jack Shaw at the ANSI X12 ASC meeting, June 9, 1986. This estimate does not include other potential savings from EDI's facilitating just-in-time manufacturing with reduced supply inventories. Shaw also reported that implementation of EDI enabled one large Eastern railroad to halve its purchasing data processing staff and is expected to cut another railroad's purchase order lead time from 10 days to 3.

[66] Irwin Greenstein, "Caterpillar Erects Paperless Network," *MIS Week*, Jan. 20, 1986.

[67] *Business Week*, op. cit., Aug. 26, 1985.

[68] "GEISCO Plans . . . ." *Washington Post*, op. cit., Sept. 29, 1986.

[69] Jack Shaw, ANSI X12 meeting on June 9, 1986.

[70] Brad Bass, "Moving Data Electronically Expedites Supply Delivery," *Government Computer News*, Jan. 30, 1987, p. 22.

Linkages in and Contrasts Between Defense-Intelligence and Other Needs

Some Linkages Between Private Sector Activities and Federal Policy.—Private industry and civilian Government agencies' interest in safeguarding their computer and communications information are becoming intertwined with Government policies even though these interests are increasingly independent of national security. The linkages between private users and the Government, and between the civil agencies and NSA, tend to blur this independence. These linkages are especially influential where NSA's technical expertise or Government certification is important, or where Government agencies, as major purchasers, tend to drive commercial equipment designs.

Although NSA's technical knowledge in high quality cryptography and cryptanalysis is acknowledged to be the cornerstone of U.S. capabilities, very little of it is unclassified. Because of this, private users depend on NSA's willingness to provide information and advice, which currently takes place, in part, in the form of NSA-certified commercial products.

Understandably, private sector users place a high value on certified, validated, and standardized safeguard products. This dependence has required considerable involvement by NBS and NSA in the absence of private sector institutions fully competent to independently develop standards and certification processes. However, NSA's plans to replace DES in 1988 with hardware modules that use secret algorithms will tend to deepen and perpetuate private sector users' dependency on NSA expertise as long as these users have no independent alternative for developing a certified, nonsecret, and exportable successor to DES.

Government agencies represent a large market for some information security products, therefore their choice of standards has a significant influence on manufacturers. According to estimates from a study conducted by the Electronic Industries Association (EIA) in cooperation with NSA, Federal and private sector budgets for information security totaled some $3 billion, split evenly between communications security and computer security.[71]

Other important linkages between Government policies and the private sector, and between defense and civilian agencies, are in the areas of security awareness, education, and assistance. During the past few years, there has been mounting confusion concerning the distinction between the roles of NBS and NSA in these areas. In addition to its Federal standards development, NBS, under its authority in the Brooks Act, as amended, participates in the voluntary activities of standards organizations and works with the private sector and civilian agencies to develop computer and computer network safeguards techniques, including security components for the open system interconnection (OSI) architecture. However, NSA, under the auspices of NSDD-145, has expanded its relationships with civil agencies, providing threat assessments and awareness briefings and advice in selecting cost-effective and appropriate safeguards. NSA reports that it has provided assistance to 36 different civil agencies and departments, plus the U.S. Senate, for diverse application areas including trade and finance, drug interdiction, law enforcement, health, agriculture, immigration, and aviation and national security,[72] as well as to Government contractors and other firms.[73]

---

[71] Of the $1.5 billion budgeted for communications security in 1986, 66 percent was budgeted by DoD, about 7 percent by other Federal agencies, and 27 percent by the private sector (including defense firms). Of the $1.5 billion for computer security, however, DoD and other Federal agencies only accounted for 13 and 11 percent, respectively, while the private sector accounted for about 75 percent. Electronic Industries Association: "COMSEC and COMPUSEC Market Study," Jan. 14, 1987.

[72] Agencies and departments that have been assisted by NSA include the United States Trade Representative, International Trade Administration, Securities and Exchange Commission, Federal Reserve Board, Department of Labor, National Narcotics Border Interdiction System, Immigration and Naturalization Service, Drug Enforcement Administration, Center for Disease Control, National Institutes of Health, Department of Agriculture, and Federal Aviation Administration. Harold E. Daniels, Jr., NSA S-0040-87, Feb. 20, 1987. Attachment 2 to Enclosure D.

[73] Ibid., Attachment 1 to Enclosure D.

Vendors of safeguard technologies and private-sector defense contractors are also closely linked to Federal information security policies and programs, such as NSDD-145. Because the new, NSA-certified encryption modules are expected to have a large, stable market among Federal agencies, vendors are unlikely to attempt development of riskier, uncertified, encryption-based safeguards. Private sector users, therefore, may be faced with limited new options if the supply of encryption-based safeguards is determined by "technology push" (from NSA) rather than "demand pull" (from unconstrained market forces).

Emerging Differences.—What is open to question is the extent to which the concerns, priorities, and needs of the defense- and national security-oriented user communities are generalizable to civilian agencies and the bulk of the private sector.

One interesting set of findings from the OTA and Ernst & Whinney surveys,[74] mentioned earlier, is based on the respondents' perceptions of who their organizations' adversaries are and illustrates an important difference between perceived Government and private sector information security needs: who the most significant adversaries are, and what level of resources they possess. Table 7 summarizes responses to a question in each survey that asked respondents to rank categories of adversaries according to how relatively important it is to protect their organizations' significant (unclassified) "company confidential" or proprietary information from them. For example, the group of 26 nongovernment individuals surveyed for OTA, predominantly nondefense Fortune 100 executives, rated foreign governments as their least important adversary.[75]

Table 7.—Overall Ranking of importance as an Adversary (Highest = 7)

	OTA survey responses[a]	
Category of adversary	Mean ranking of category	Fraction of responses ranking category #1 or #2
Your competition	6.7	92%
Some of your internal employees	4.8	31
Foreign governments	3.1	4
Your suppliers	4.1	15
Your customers	4.9	27
Public interest groups	4.0	19

[a] All respondents were non-government

	Ernst & Whinney survey non-government responses[b]	
Category of adversary	Mean ranking of category	Fraction of responses ranking category #1 or #2
Your competition	6.5	89%
Some of your internal employees	4.9	43
Foreign governments	3.9	30
Your suppliers	4.1	11
Your customers	4.7	35
Public interest groups	3.9	15

[b] Between 200-300 out of a total of 421 non-government respondents ranked each category of adversary: the rest did not rank that category

	Ernst & Whinney survey Government responses[c]	
Category of adversary	Mean ranking of category	Fraction of responses ranking category #1 or #2
Your competition	4.1	35%
Some of your internal employees	5.3	53
Foreign governments	6.1	74
Your suppliers	4.3	24
Your customers	4.5	34
Public interest groups	5.0	48

[c] Between 26-49 out of a total of 141 government respondents ranked each category of adversary: the remainder did not rank that category

Similarly, the larger sample of non-Government respondents surveyed by Ernst & Whinney ranked foreign government adversaries lowest overall. Instead, both non-Government groups considered their competition as the most important single adversary, followed by customers and some internal employees, and then by suppliers, public interest groups, and foreign governments. The Government respondents surveyed by Ernst & Whinney considered foreign governments (perhaps analogous to "your competition" for businesses) to be the most important adversary, followed by some internal employees, public interest groups, and the other categories. An important difference between business competitors and foreign government adversaries is, obviously, the level of resources that each type could deploy to gain access to information.

---

[74] The OTA computer security survey was conducted in October 1986, at a meeting of Palmer Associates. The 26 respondents to the questionnaire were data processing audit vice-presidents and data processing audit directors of Fortune 500 companies. Ernst & Whinney, "OTA Computer Security Survey," OTA contractor report, Nov. 7, 1986.

Ernst & Whinney conducted a separate survey in November 1986 at the 13th annual conference of the Computer Security Institute. About 500 attendees responded to this self-administered survey, most of whom had responsibility for computer security functions. The data were made available to OTA in February 1987.

[75] One of the OTA survey respondents noted that his firm was most concerned with protecting information from foreign governments; another was concerned with protecting confidential customer information from the U.S. Government.

The Electronic Industries Association market study mentioned earlier also found "widely different perceptions of the threat to information systems and this results in different and often conflicting and competing security requirements . . ." The study notes a national security perspective that focuses on external threats while others' perceptions are of internal sources as the principal threat.[76] It also notes that businesses and civilian agencies attached considerable importance to the cost of safeguards and their effect on operations.

Other differences (and similarities) between current Government and private sector information security priorities are suggested by a survey question asking respondents to list their organizations' "top-priority" computer-security and information-security concerns. These responses are summarized in table 8. Although the same types of concerns are mentioned by Government and private sector respondents, their relative priorities are different.

An important effect of these perceptions and priorities is on the users' decisions concerning the use and choice of safeguards.

Another interesting finding from both the OTA and Ernst & Whinney surveys was the relatively low level of perceived impact (as of Fall 1986) from NSDD-145 on non-Government organizations' safeguarding of unclassified information. Table 9 summarizes responses to a survey question about the impacts of NSDD-145. Almost three-quarters of the respondents (all non-Government) to the OTA survey and almost half of the non-Government Ernst & Whinney survey respondents felt that NSDD-145 had had no impact on their organizations' safeguarding of unclassified information. Moreover, fewer than 10 percent of the respondents to the OTA survey and fewer than 30 percent of the non-Government respondents to the Ernst & Whinney survey considered that the directive had impacted their firms' security practices for unclassified information "somewhat" or "greatly."[77] By contrast, the Government respondents in the Ernst & Whinney survey reported much higher levels of impact overall, with only one-quarter reporting no impact from NSDD-145 on unclassified information security and almost 60 percent reporting that the directive had impacted their organizations' unclassified information security at least somewhat.

More than two-thirds of both the OTA survey respondents and the non-Government respondents to the Ernst & Whinney survey felt that their firms' information and data security measures were at least fairly adequate to meet their needs. What is somewhat surprising is the relatively low percentages of these firms' total information and computer security expertise attributed to Government-sponsored assistance programs, conferences, and training programs. Only 2 of the 26 OTA survey respondents indicated that even a small percentage of their firms' information and data security expertise came directly from Government assistance programs. This low percentage is likely due to the composition of the Palmer Associates group surveyed and is in marked contrast to what one might expect

---

[76] Electronic Industries Association, "COMSEC AND COMPUSEC Market Study," Jan. 14, 1987. This study was based on 75 interviews, 64 of which were with Federal agencies, including 39 having defense and intelligence missions.

[77] Two firms in the OTA survey indicated that they had implemented encryption or scrambling to protect sensitive communications in response to NSDD-145, and one of these firms also implemented access control software, passwords, and acquired special communications channels.

Table 8.—Top-Priority Computer and Information Security Concerns Mentioned by Respondents

OTA survey group (non-government)	Ernst & Whinney non-government group	Ernst & Whinney Government group
Data security/data integrity	Network security	Contingency planning/disaster recovery
Network security	Data/information classification and security	Data/information classification and security
Contingency planning; training	Micro/PC security	Network security
Quality security throughout firm; telecommunications links; internal hacking	Dial-up security/communications	Micro/PC security

SOURCE: Data from surveys conducted by Ernst & Whinney in October and November 1986.

Table 9.—Perceived Impacts From NSDD-145 (Fall 1986)

Question: "On September 17, 1984, President Reagan signed National Security Decision Directive 145 (NSDD-145), the National Policy on Telecommunications and Automated Information Systems Security. This policy has led to much more active involvement by the National Security Agency and the National Computer Security Center in providing advice to business and industry. How has NSDD-145 impacted your organization in safeguarding information that is not classified for purposes of national security?"

	Survey responses			
Response	OTA survey total responses to question (all non-government) (23)	Ernst & Whinney total responses to question (486)	Ernst & Whinney non-government responses (364)	Ernst & Whinney government responses (122)
Not at all	74%	41%	46%	25%
Very little . .	17	25	27	18
Somewhat . . .	9	24	21	33
Greatly	0	11	6	24

SOURCE: Data from surveys conducted by Ernst & Whinney in October and November 1986.

from an alternative group composed of defense contractors, computer firms, or firms producing security products for the Government market. In fact, only two of the respondents to the OTA survey indicated awareness of any specific Government-sponsored information and assistance programs. Of the 22 individuals responding to a question concerning their perceptions of the helpfulness of Government guidelines, 17 answered "not at all," while 5 said these had been "somewhat" helpful to their organizations. The respondents who did find Government guidelines helpful cited the NBS Federal Information Processing Standards (FIPS), including DES, as well as guidelines for protecting privacy-related and classified information.

Differences Between Military and Civilian Computer Security Models.—The debate about how well the NSA's Orange Book computer security standards and evaluated products program will serve the needs of civilian agencies and private businesses is receiving increased attention within the computer security community. One of the most crucial aspects of the debate concerns the security policy underlying the Orange Book criteria, the mechanisms needed to enforce security policy, and how well these match the security policies (and associated mechanisms) that are common in commercial practice. According to computer security experts at NSA, for example, the National Computer Security Center (NCSC) has worked —and continues to work—"hand in glove" with the civilian agencies to understand their needs and provide appropriate computer security solutions[78] and, moreover, products that have been evaluated by NSA and that have received

---

[78] Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, p. 7 of Enclosure 2.

B- and C-level ratings are being used in the private sector (some of these, such as RACF, ACF2, and Top Secret, were developed well before the Orange Book was published but have been modified to meet Orange Book standards). Other experts disagree with this position, and argue that the security policy and mechanisms specified in the Orange Book do not meet important needs in commercial data processing.

Among the latter group are David D. Clark (MIT Laboratory for Computer Science) and David R. Wilson (Ernst & Whinney). In their paper, "A Comparison of Commercial and Military Computer Security Policies,"[79] they present a security model based on commercial data processing practices and compare the mechanisms needed to enforce this model's rules with those needed to enforce the (lattice) model of security embodied in the NSA criteria. Other experts have also offered criticisms of the Orange Book's applicability to business needs. However, a brief summary of the Clark and Wilson paper, offered here as an example, points out some of the main points of criticism.

According to Clark and Wilson, the "military" (NSA/DoD) security policy is really a set of policies designed to control classified information from unauthorized disclosure or declassification. Mechanisms used to enforce this security policy include mandatory labeling of documents or data items, assigning of user access categories based on security clearances, generating audit information, etc. The higher-level security policies include mandatory checks on all read and write transactions; these mandatory controls constrain the user so that any action taken is consistent with the security policy. In addition to these mandatory controls, discretionary controls can be used to further restrict data accessibility (e.g., "need to know" controls), but, say Clark and Wilson, these cannot increase the scope of security controls in a manner inconsistent with the underlying multi-level classification concept.

By contrast, Clark and Wilson assert that what underlies commercial data processing security practices is the prevention of fraud and error and, therefore, that a "commercial" security policy should address integrity rather than disclosure. Some of the mechanisms to enforce this type of policy are common with those for the military model (for example, user authentication), while others are very different. Among these others, Clark and Wilson identify two principal mechanisms: the well-formed transaction (in which a user can manipulate or record data in constrained ways that preserve or ensure the integrity of the data—analogous to a paper-and-ink accounts book in which correction entries, rather than erasures, are made); and separation of duty among employees (in which the user permitted to create or certify a well-formed transaction may not be permitted to execute it—analogous to double-entry bookkeeping in which a check for payment must be balanced against a matching entry in the accounts-payable column). Separation of duty is a fundamental principle of commercial data integrity control, and is considered effective except in the case of collusion among employees.

In their paper, Clark and Wilson conclude that the integrity mechanisms inherent in the commercial security model differ from the mandatory controls in the military (nondisclosure) security model in important ways, and controls based on the military model are not sufficient to enforce the commercial (integrity) model. They then introduce a more formal model for data integrity in computer systems, based on the use of constrained data items and transformation procedures for enforcing an integrity policy. Comparing this model with other integrity models, Clark and Wilson argue that their model, unlike the Orange Book standard, is applicable to a wide range of integrity policies.

By early 1987, debate on the general applicability of the Orange Book criteria and development of alternative models of computer and information security had developed to the extent that plans were made for an invitational Workshop on Integrity Policy for Computer

---

[79] David D. Clark and David R. Wilson, "Commercial Security Policies," *Proceedings, 1987 IEEE Symposium on Security and Privacy*, Oakland, CA, Apr. 27-29, 1987.

Information Systems, organized by Ernst & Whinney and co-sponsored by the Institute for Electrical and Electronic Engineers, the Association for Computing Machinery, NBS, and NSA's National Computer Security Center (NCSC), to address military versus commercial security policy issues. The workshop is scheduled to be held in late 1987.[80]

Civilian Agency Actions.—In addition to the NBS activities described earlier, related to DES, FIPS publications, and voluntary standards development, there are other civilian agency activities related to safeguarding electronic information. (An earlier OTA report surveys civilian agency programs for computer security.)[81] The Treasury Department, for example, requires the use of safeguards for information systems that handle sensitive, as well as classified, information.[82] All Federal electronic fund and securities transfer systems must also have safeguards in place by June 1988. The requirement applies to all Federal agencies (except DoD, which has its own policy) and to wholesale banks that do business with Treasury and use the Federal Reserve System as the interface.[83] The Treasury Department Order (TO 106-09) requires that authentication measures conform to the American National Standard Institute (ANSI) X9.9 standard "or equivalent authentication technique."[84] According to Department of Treasury officials, the DES "is and will remain fundamental to the Department's security strategy for the foreseeable future."[85] Treasury has announced that technology to secure Federal electronic fund transfers (EFTs) must be compatible with systems used by the Federal Reserve System and the commercial banking community. Specifically:

- Treasury will continue to support and implement ANSI financial standards as the common method for securing Federal EFTs and will only transition from the current (DES based) ANSI standards to any new ANSI standard (not based on DES) if the transition is based on "sound business decisions and security needs."
- Treasury will rely on NSA's commitment, of November 12, 1985, that DES will be supported indefinitely for the financial community.
- Treasury will rely on NBS to continue to validate DES chips.
- Treasury will continue to certify equipment and techniques for Federal use to provide authentication/encryption and automated key management for EFTs.
  Treasury will continue to develop, in conjunction with NBS, automated test beds/bulletin boards so that NBS can validate successful hardware and software implementations of ANSI financial standards.[86]

The Federal Reserve System publicly expressed its commitment to electronic data security in early 1985, when it announced specific plans to enhance its electronic payment services in order to increase their security. The Federal Reserve is a highly-visible participant in the Nation's electronic payments system, both as an operator (performing electronic fund and securities transactions, serving as an automated clearinghouse, etc.) and as a regulator. In its role as an operator, the Federal Reserve must protect its value transactions; as a regulator, the Federal Reserve intends that its security and reliability standards serve as models for depository institutions to emulate in securing their own electronic payments operations.

---

[80] Information on workshop from David Wilson and Jenny Sobrasky (Ernst & Whinney), private communications with OTA staff May 5-6, 1987, and from an IEEE press release (May 1987).

[81] OTA-CIT-297, op. cit.

[82] Department of the Treasury, Directives Manual, Information Systems Security, Ch. TD 81, Section 40, Apr. 2, 1985.

[83] Department of the Treasury, *Directives Manual*, "Electronic Funds and Transfer Policy—Message Authentication," TD 81, Section 80, Aug. 16, 1984. Superceded by: Department of the Treasury. "Electronic Funds and Securities Transfer Policy—Message Authentication and Endorsed Security," TD816-02, Oct. 3, 1986, TD/16-02 is authorized by Treasury Order 106-09, Oct. 2, 1986.

[84] Department of the Treasury Order #106-09, "Electronic Funds and Securities Transfer Policy—Message Authentication and Enhanced Security," Oct. 2, 1986.

[85] J. Martin Ferris, Security Programs, Department of the Treasury, Washington, DC, letter to OTA staff, Dec. 16, 1986.

[86] Ibid.

The Federal Reserve's plans include encryption of depository-institution connections; as of late 1986, over 60 percent of these were encrypted and the Federal Reserve plans to have almost 100 percent of them encrypted by the end of 1987. In addition, the Federal Reserve is currently testing the use of message authentication within the Federal Reserve environment.[87] The National Bureau of Standards is providing technical support to the Federal Reserve.

Technical Standards Development

Technical standards are important for a number of reasons. Among other things, they help to aggregate markets by improving the uniformity, interoperability, and compatibility of vendors' products.

Federal Agency Participation.—NSA and NBS activities in the development of standards have been noted earlier. Other agencies involved in the development and promulgation of regulations and standards include the Office of Management and Budget, the General Services Administration (GSA) and DoD's National Communications System (NCS). GSA promulgates Federal procurement regulations generally, including telecommunications, and has delegated its responsibilities for producing and coordinating communications standards to NCS, which has issued DES-related standards for telecommunications security and interoperability.

NBS has had considerable success during the past decade in developing a variety of standards for information security, as well as by publishing dozens of guidelines. Known as Federal Information Processing Standards (FIPS), NBS standards apply to civilian agencies. Several have also become the basis for standards developed or adopted by NSA and by private standards-setting organizations such as ANSI, the ABA, and the International Organization for Standardization (ISO).

One of the earliest of these national standards, DES, (FIPS 46, released in 1977) is discussed in appendix C. DES, which is now produced in hardware and software both in the United States and overseas,[88] has been adopted by ANSI in a number of its technical standards, and was considered for use as an international standard by an ISO technical committee in 1986, as discussed later.

Private Sector Participation.—Active participation in the development of technical standards for information safeguards is another indication of the current and future needs of business users. ANSI has had active participation from several dozen major corporations, including banks, equipment vendors, and (more recently) other manufacturers. For example, several large U.S. banks and the American Bankers Association (ABA), the Canadian Bankers Association, and about 30 vendors are among the participants in developing standards of interest to the banking community, in addition to NBS, the Treasury Department, and NSA. Suppliers and users of sophisticated safeguards such as biometrics and other technologies not based on cryptography have acted more independently of the Federal Government, sometimes in the absence of technical standards. Defense agencies are major consumers of these products, but the Federal Government does not enjoy the near monopoly in technical expertise that it has in cryptography. In the area of biometrics, the International Biometric Association was formed in 1986 to address industry issues, including establishing a testing and standards program.

Most large corporations have developed or are developing their own information safeguard policies. For example, the Chemical Bank of New York, which has more than 250 branches, has developed its own policies and a security training program for bank employees.[89] The bank's policies, published in 1985, define security and custodianship responsibilities in the bank's distributed operating environment and govern the transfer of information in hard copy and electronic forms to protect the bank's information service and data assets. The bank has developed a software package that it uses to train branch officers to perform risk assessments for their local offices and to implement the corporate security standards. By late 1986, the software package had been used in at least 30 Chemical Bank locations.[90]

---

[87] Jack Dennis, Assistant Director of Federal Reserve Bank Operations, Washington, D.C. Personal communication with OTA staff, Aug. 26, 1986 and letter, Dec. 17, 1987.

[88] Federal Government certification applies only to implementations of DES in electronic devices.

[89] "Corporate Data Security Standards," Chemical Bank (Chemical New York Corp.), 1985; also Presentation by Joan Reynolds (Chemical Bank), panelist in "Guidelines and Standards Panel," Ninth National Computer Security Conference, Gaithersburg, MD, Sept. 16, 1986.

The Small Business Computer Security and Education Act (Public Law 98-362) provided another mechanism for private sector participation in developing information security standards and guidelines. Passed in July 1984, the act set up a 10-member Small Business Computer Security Advisory Council to advise small businesses on the vulnerabilities to misuse of computer technologies (especially in distributed network environments) and on the effectiveness of technological and management techniques to reduce these vulnerabilities. It also develops guidelines and information to assist small businesses and plans to distribute written materials, including a small business guide to computer security (to be published by NBS) in mid-1987.[91] A report to Congress will be issued by December 1987.

The Applied Information Technologies Research Center (AITRC) represents yet another private sector approach to meeting information safeguard needs. A consortium of scientific, technological, and business organizations based in Columbus, Ohio, AITRC is part of this State-supported program. It was supported by an initial State grant of $1.4 million. Its industrial members include leaders in online information services, and one AITRC project is developing techniques for secure access to private and subscription databases. In the fall of 1986, AITRC was licensing a low-cost, credit card device for remote user identification.[92]

Technical Standards Bodies.—Another indication of the variety of users' needs and demands is provided by the activities of the technical standards-making bodies. Users and vendors in the banking and information processing communities, and in civilian Government agencies, have been working with considerable success for the past decade to develop standards to meet their needs for improved information safeguards. These groups recognize that standards establish common levels of cryptographic-based security and interoperability for communications and data storage systems.[93]

The leading information standards-making organizations in the United States have been the Institute for Computer Sciences and Technology at NBS, the American National Standards Institute (ANSI), and the American Bankers Association (ABA), as noted earlier. The International Organization for Standardization (ISO), develops voluntary standards for international use. Through these bodies, users and vendors are setting the stage for improving the integrity and security of computer and communications systems world-wide.

The American National Standards Institute (ANSI) serves as a national coordinator and clearinghouse for information on U.S. and international standards. It is the central nongovernment institution in the United States for developing computer, communications, and other technical standards for industry. ANSI members represent a broad range of industries and technical disciplines. NBS is a member of many ANSI committees, including those dealing with message authentication and encryption; other Federal agencies including Treasury and NSA also have memberships. ANSI serves as the U.S. representative to the International Organization for Standardization (ISO).

---

[90] Personal communications between OTA staff and Denise Ulmer, Chemical Bank of New York, Sept. 25, 1986.

The software package, RiskPac$^{\text{TM}}$, is also being marketed commercially through Chemical Bank Information Products and Profile Analysis Corporation, Ridgefield, Connecticut. Personal communication between OTA staff and Peter S. Brown, Profile Analysis Corp., Sept. 25, 1986.

[91] Information provided by Peter S. Brown, chairman, Small Business Computer Security Advisory Council, Sept. 25, 1986.

[92] Sources: *Information Hotline*, July-August 1986, pp. 6-7; and personal communication between OTA staff and Richard Bowers, AITRC, Sept. 8, 1986.

[93] D. Branstad and M. Smid, "Integrity and Security Standards Based on Cryptography," North Holland Publishing Co., Computers & Security 1 (1982) CAS00043 [NC]. Also, see Organization for Economic and Co-operative Development, Committee for Information, Computers, and Communications Policy, "Standards and Standard-Setting in Information Technology-Stakes, Strategies, and International Implications," Sept. 5, 1985.

These organizations are structured internally into committees, technical committees, and working groups to accommodate the special interests of their members and to provide a narrow focus, where needed, for developing particular standards and guidelines. Among the structures related to information security are:

- ANSI's X3 (Information Processing Systems) Committee, which includes the encryption technical committee; and ANSI's X9 (Financial Services) Committee, which includes the financial institution message authentication working group, the financial institution key management committee, and the bank card security working group (focusing on personal identification number, management, and security);
- ABA, which focuses on financial transactions safeguards, including encryption and message authentication; and
- ISO's Technical Committee 97 (TC-97) and its various subcommittees and working groups, which are responsible for developing standards for information processing systems; and Technical Committee 68, which has similar responsibilities for the financial community.

These bodies make extensive use of one another's work, often adopting the other's standard intact or with modifications. Table 10 shows the progress being made in the development of standards and guidelines, as well as many of the contributions of different civilian institutions.

The interests of many developed countries in establishing an international standard for cryptography have recently culminated more than 5 years of deliberation in the ISO. In December 1985, an ISO technical subcommittee recommended that DES be adopted as an international standard.[94] Any standard adopted by the ISO would likely be used throughout much of the developed world to safeguard communication and computer systems. Disagreements within the U.S. delegation (between NSA and the business community members of ANSI) led the U.S. delegation to abstain during the ISO vote on DES.[95] ANSI, in mid-1986, recommended to ISO that cryptographic algorithms not be the subject of international standardization. This change from ANSI's previous position probably came in response to NSA suggestions.[96] Several months later, the ISO Technical Committee TC97 announced the withdrawal of the proposed DEA-1 standard.[97]

Some of the other nations involved in the ISO deliberations have proposed their own algorithms as alternatives to DES.[98] This proposal may give credence to what many believe, i.e., that not only can other nations offer encryption algorithms for international use, but that future encryption services will be decided based on international commercial needs. The

---

[94] Vincent McClellan, "The Pentagon Couldn't Defeat IBM in Battle Over DES Standard," *InformationWeek*, Feb. 24, 1986, pp. 24-27.

[95] Ibid., pp. 24-27.

[96] During a meeting with NSA officials in June 1986, OTA staff were advised that since most private sector foreign representatives to the ISO have close ties with their governments, the final ISO decision on whether to adopt the DES could be decided prior to ISO voting through private negotiations among governments. Furthermore, NSA officials have stated that NSA is not in favor of DES (or any one algorithm) being used as an international encryption standard. Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, p. 2 of Enclosure 2.

Critics of NSA are sometimes inconsistent. For example, there was speculation that the real reason that NSA opposes DES, or any other algorithm, as an international standard is that it would damage NSA's signals intelligence operations or benefit criminal elements. On the other hand, others speculate that DES is easy for a government intelligence agency to decipher.

However, according to one NSA executive, there is no evidence that anyone has yet found a way to break the DES. But, because DES has come into such widespread use, it may become an attractive target for just such attempts. OTA staff meeting with Harold E. Daniels, Jr., NSA, Aug. 13, 1986.

[97] Vincent McClellan, "The Pentagon Couldn't Defeat IBM in Battle Over DES Standard," *InformationWeek*, Feb. 24, 1986, pp. 24-27.

[98] Ibid.

Table 10.—Selected Civilian Technical Standards for Safeguarding Information Systems

Standard/guideline	Developer/year	Principal and other users/uses
Data Encryption Standard (DES) (FIPS PUB 46)	NBS (1977)	U.S. Government (computer and communication security); increasing use in private sector
DES Modes of Operation (FIPS PUB 81)	NBS (1980)	U.S. Government (key management, character transmission, packet transmission, voice)
Key Notarization System (U.S. patent 4,386,233)	NBS (1980)	U.S. Government (notarized identification of originator and receiver of secure message or data file); also used in banks
Guidelines for Implementing the DES (FIPS PUB 74)	NBS (1981)	U.S. Government (general DES user information)
Computer Data Authentication (FIPS PUB 113)	NBS (1985)	U.S. Government (authentication code for data integrity in ADP systems and networks); some use in private sector
Password Usage Standard (FIPS-112)	NBS (1985)	U.S. Government (identifies ten security factors for a password system)
General Security Requirements for Equipment Using DES (FS-1027)	GSA (1982)	U.S. Government (physical and electrical security of DES devices)
Interoperability and Security Requirements of the DES in the Physical Layer of Data Communications (FS-1026)	GSA (1983)	U.S. Government
Data Encryption Algorithm (DEA)	ANSI X3.92 (1981)	U.S. industry (voluntary standard, DEA is ANSI terminology for the DES)
Data Link Encryption Standard	ANSI X3.105 (1983)	U.S. industry
DEA Modes of Operation	ANSI X3.106 (1983)	U.S industry
Financial Institution Message Authentication (wholesale)	ANSI X9.9 (1983)	Wholesale banks (message authentication); industry (electronic procurement message authentication)
Personal Identification Number (PIN) Management and Security	ANSI X9.8 (1982)	Retail banks (DEA encryption of PINs; retailers (computer access control)
Financial Institution Key Management	ANSI X9.17 (1985)	Wholesale banks and industry (cryptographic keys for encryption and message authentication)
Financial Institution Message Authentication (Retail)	ANSI X9.19 (1986)	Retail banks (message authentication using DEA)
Financial Institution Encryption of Wholesale Financial Messages	ANSI X9.23 (draft)	Wholesale banks and industry
Management and Use of PINs	ABA (1979)	Banks (general guidance)
Protection of PINs in Interchange	ABA (1979)	Banks (general guidance)
Key Management Standard Doc. 43	ABA (1980)	Banks (general guidance)
Data Encryption Algorithm (DEA-1)	ISO (1986)	Proposed international version of DES (FIPS-46); withdrawn by ISO Technical Committee TC97.
Modes of Operation of DEA-1	ISO/DIS 8372	Draft international standard has been approved (title may change due to withdrawal of proposed DEA-1 standard)
Data Link Enciphering Standard	ISO/DIS 9160	Draft international standard, version of ANSI X9.105
Message Authentication	ISO/DIS 8730	Draft international standard for message authentication; Part 1 specifies the DEA-1 algorithm, Part 2 specifies the MAA algorithm
Public Key Encryption Algorithm and Systems	ISO/DP 9307	Draft proposal for standards (may be stricken)
Banking: Key Management (wholesale)	ISO/DIS 8732	Draft international standard for wholesale banks

SOURCE: Office of Technology Assessment, 1987 trend toward the standardization of encryption-based safeguards, principally for improving message integrity (virtually all of which are currently based on DES, often in conjunction with public-key cryptography) suggests that within a few years major segments of the world's businesses will have standardized information safeguards where needed.

Second, these trends indicate that the role of the U.S. Government is shifting from that of the principal developer of safeguard standards in the early 1970s to a more limited role of one participant among many, although with continuing and important responsibilities.

Inherent Diversity of User Needs

Decisions on arcane technical standards, originally based on national security concerns, have already begun to be influenced by various, growing nondefense interests in the United States and worldwide. If safeguard products meeting Federal standards for certification do not fully meet commercial needs, then users are likely to seek greater independence from the Federal Government. Some movement in this direction is already taking place, as evidenced by: unpublicized plans in 1987 of the U.S. banking community to bypass NSA's secret algorithms; growing commercial interest in proprietary public-key algorithms, which have no Federal standard but meet users' needs for electronic key distribution and digital signatures; and, the workshop on Integrity Policy for Computer Information Systems, planned for late 1987, which will focus on military v. commercial security models.

The foregoing description of various users' needs, and actions that Government and private sector groups have undertaken to meet them, serves to point out the inherent diversity and heterogeneity of users' needs for information safeguards. Within the Federal Government itself, for example, different requirements exist among defense and civilian agencies, and even between classified and unclassified applications (such as food service or routine procurement) within DoD. The private sector is no more uniform in its needs, attitudes, and perceptions. In order to understand the differences in each user's requirements, priorities, and perceived risks and threats, information such as the following must be evaluated by each user:

- What are the user's major concerns? For example, what is the relative priority for various types of information for integrity versus confidentiality, versus reliability and continuity of service?
- What sensitive information may warrant better safeguards than are now provided?
- Who are the adversaries that need to be protected against (employees, competitors, foreign governments) and the resources they are likely to use?
- What are the likely consequences (financial, embarrassment, privacy) of different types of losses? What has been the loss experience to date?
- What are the decision criteria (costs and benefits for bolstering safeguards, required by law, risk aversion)?

Responses to these and other questions help to define the user's needs for safeguards and are likely to be different from one user to another, even when they are in the same general business. A defense contractor bound by DoD policies and regulations for safeguarding classified information from foreign adversaries, for example, can recover the costs of safeguards from the Government. This is a very different situation than that of a large retailer who needs to authenticate thousands of transactions per day, with emphasis on service delivery, costs, data integrity, and protection against dishonest employees and customers. And, the retailer's needs bear little resemblance to the bank manager's requirement to show that he has exercised due care in safeguarding the bank's assets.

Chapter 6 focuses on some of the major laws and policy directives concerning information security. In tracing the development of public policy, it seeks to provide insights into the question: "How did we get where we are today?"

Chapter 6

Major Trends in Policy Development

CONTENTS

Page

Findings 131

Introduction 131

The Evolution of Federal Policy for Safeguarding Unclassified Information in Communications and Computer Systems 135

- Executive Branch Activities in Information Security 135
- Computer Security 136
- Communications Security 137
- Definition of Sensitive Information 139
- Policy Development in Congress 140

Government Controls on Unclassified Information 141

- Controls Through Legislation 141
- Executive Branch Directives and Other Restrictions 143

The Environment for Policy Development 145

- The Early Environment 145
- The Changing Environment and Federal Policies 145
- The Current and Future Environment 146

Current Congressional Interest 147

Tables

Table No. Page

11. Selected Government Policies Related to Controls on Information Flows: A Context for Electronic Information Security 132
12. Government Actions Affecting the Security of Information in Computer and Communications Systems 134
13. Committees Guiding the Implementation of NSDD 145 139

Chapter 6

Major Trends in Policy Development

FINDINGS

- Federal policy limiting the disclosure of information has expanded over the last decade to include growing concern for protecting unclassified, but sensitive information, such as that in commercial and Government databases. As part of this process, the role of the defense and intelligence communities has also expanded and "national security," as a criteria for non-disclosure, is being interpreted more broadly.
- Federal policies on information security are creating tensions with broad national interests and, in contrast with earlier times, can no longer be isolated from them.
- Most recent Federal policies on information security are based principally on national security concerns. Now that information security is becoming important to commerce, more broadly based policies will be more appropriate.
- The National Security Agency (NSA), in carrying out its role under National Security Decision Directive (NSDD-145) to develop computer and communications security standards for use by Government and industry, is involved in two policy conflicts. One conflict involves responsibilities for developing security standards, with the National Bureau of Standards (NBS) charged by the Brooks Act of 1965, as amended, and NSA having overlapping responsibilities under NSDD-145. The second is a continuing, inherent conflict between NSA's mission to perform signals intelligence and its efforts to develop computer and communications safeguards for widespread nondefense use.

INTRODUCTION

Policy for the security of electronic information has developed in recent years in a setting of diverse interests. These interests have included national security and the separation of powers for governmental policymaking, as well as civil liberties, including personal privacy, and commercial needs for improved information safeguards. The current tensions in information security policy reflect all of these influences. To a large extent, these tensions have their basis in different views within Government of overall national interests and the central historical role of the Government, particularly the Department of Defense (DoD), in developing technology and setting policies for safeguarding electronic information.

This chapter provides a brief review of two of these influences:

- the context of Government controls on unclassified information that has evolved during the past few decades, and;
- the progression of prior policies concerning the privacy and security of electronic information that have led to today's policies.

Policies designed to keep electronic information secure developed historically largely in the context of protecting national security. One of the important ways that has been used to limit potential damage to the nation's security is through controls on the dissemination of information. Federal limitations, dating to before the turn of the century, sought to prevent the disclosure and distribution of militarily sensitive, Government-owned or -controlled information.[1]

Traditionally, information protected for national security reasons has been limited to military and diplomatic categories. Since the 1940s, a number of laws have been passed and presidential directives issued that have gradually expanded the range of information deemed vital to U.S. national security. Controls have been placed on data relating to, for example, atomic energy, space programs, and a variety of other technologies. (See table 11.) Similarly, efforts have been made to keep intelligence sources and methods secret and there have been discussions on whether controls might be warranted for satellite imagery gathered for the news media.[2]

At the same time, the medium of information that is to be controlled—i.e., oral, print, photographic, or electronic—has also expanded. The setting for the transfer of controlled information has become irrelevant, whether through the export of products or services, sales presentations, university laboratories and classrooms, or scientific or trade conferences.

Against this backdrop, computer and communications systems are among the media for controlling the transfer of such sensitive information. Concern for their vulnerability to penetration, particularly by foreign intelligence entities, has resulted in pressure to increase the security of these systems.

A second context that affects Government controls on information concerns the respective roles of and occasional conflicts between the executive and legislative branches in setting policy when national security is at stake.[3] The history of this controversy has its origins in the drafting of the Constitution and it continues to raise complex issues for both branches. Since the beginning of the Cold War in the mid-

Table 11.—Selected Government Policies Related to Controls on Information Flows: A Context for Electronic Information Security

1940s:
- Atomic Energy Act[a]
- Export Control Act[b]
- National Security Act[c]
  - —establishes the Central Intelligence Agency

1950s:
- Invention Secrecy Act[d]

1960s:
- Export Administration Act of 1969[e]

1970s:
- Arms Export Control Act of 1976[f]
- PD/NSC-24[g]
  - —safeguard sensitive Government information in communications systems

1980s:
- Defense Authorization Act, 1984[h]
  - —controls on military and space technical data
- NSDD 189[i]
  - —clarify controls on basic research data
- NSDD 145[j]
  - —safeguard sensitive information in computer and communications systems

Recent reports:
- Air Force study of foreign access to commercial databases[k]
- Soviet acquisition of Western technology[l]
- Senate report on counterintelligence[m]

[a] Atomic Energy Act of 1946 (60 Stat. 755)

[b] Export Control Act of 1949 (63 Stat. 7).

[c] National Security Act of 1947 (50 U.S.C. 403, Sec. 403). This Act also provides standards for classifying and safeguarding information for the protection of national security, notably intelligence sources and methods.

[d] Invention Secrecy Act of 1951 (U.S.C. 181-188).

[e] Export Administration Act of 1979 (50 App. USC 2401-2413), as amended, 1979, 1981, 1985.

[f] Arms Export Control Act of 1976 (22 USC 2571 et seq.)

[g] Presidential Directive/National Security Council-24, (PD/NSC 24), Telecommunications Protection Policy (unclassified excerpts, dated Feb. 9, 1979), Nov. 16, 1977 (classified).

[h] Department of Defense Authorization Act, 1984, P.L. 98-94, Sept. 24, 1983, Section 1217, Authority to Withhold from Disclosure Certain Technical Data (10 U.S.C. 140c).

[i] NSDD 189, National Policy on the Transfer of Scientific, Technical, and Engineering Information, Sept. 21, 1985.

[j] National Security Decision Directive 145 (NSDD 145), Policy on Telecommunications and Automated Information Systems Security, Sept. 17, 1984.

[k] "The Exploitation of Western Data Bases," Report of the Air Force Management Analysis Group, (Secret), June 30, 1986.

[l] "Soviet Acquisition of Militarily Significant Western Technology: An Update," Department of Defense, September 1985.

[m] "Meeting the Espionage Challenge," Senate Select Committee on Intelligence, Report No. 99-522, Oct. 3, 1986.

---

[1] "The Evolution and Organization of the Federal Intelligence Function: A Brief Overview (1776-1975)," Supplementary Reports on Intelligence Activities, Book 6, Senate Select Committee to Study Government Operations, Report 94-755, Apr. 23, 1976.

[2] U.S. Congress, Office of Technology Assessment, *Commercial Newsgathering From Space—Technical Memorandum*, OTA-TM-ISC-40 (Washington, DC: U.S. Government Printing Office, May 1987).

[3] Harold C. Relyea, "National Security and Information," *Government Information Quarterly*, vol. 4, No. 1, 1987, pp. 11-28.

1940s, the debate over the roles of the two branches has included such topics as atomic energy, satellite communications, and the funding of research in fields such as electronics and supercomputers and of the roles of the military v. civilian agencies.

The controversy over policymaking responsibilities within the Federal Government has a direct bearing on Federal policy in information security primarily because it influences the scope of national interests to be embraced in such policies and, in that process, the priorities emphasized. For example, one view of national interests places priority on military advantage and defense capability, with national security often being promoted through reliance on secrecy and Government controls. Advocates of this view accept the idea of Government control of access to information in the greater interest of national security. The other viewpoint focuses on the United States as a free and open society in which access to information, for realizing scientific, economic, and intellectual achievement, should be subject to only minimal Government control when there is clear justification.

In addition, the process by which policy is developed is becoming increasingly important as the range of national interests affected expands beyond national security concerns and, consequently, as tensions among competing objectives are created. Policymaking in Congress tends to be an open process, in contrast with the often closed process underlying past executive branch policies concerning communications and computer security.

Federal policy on electronic information security has also been shaped by concerns for privacy and civil liberties. Laws have been passed limiting warrantless Government wiretaps and prohibiting eavesdropping on others' private communications or gaining unauthorized access to computer systems. This path of Federal policymaking, which has its origins with the Communications Act of 1934, has gained momentum during the past two decades independent of concerns for foreign intelligence gathering.

As a consequence of these various influences, most of which have ramifications that extend well beyond information security, policy formulation has followed at least two interdependent paths, at times initiated by Congress and at other times by the executive branch. The resulting policies, are highlighted in table 12. In this process, however, there has been a growing influence of defense and intelligence interests in shaping policy for the security of unclassified electronic information.

Until recently, Federal policies on electronic information security, whatever their objectives, have not raised tensions. What is different about the policies of the 1980s, however, is that some of these have begun to affect segments of the private sector more significantly. In contrast with earlier policies, which had negligible influence on nondefense businesses or private citizens, recent policies have tended to impose added burdens on some businesses, to raise concerns for new restrictions on private sector access to unclassified, but sensitive information, and to interject an intelligence agency in normal business operations. (See ch. 5.)

Some of the key questions that arise are: where is policy for the security of electronic information leading? can the current issues be resolved? what new issues might arise? The review of the evolution of policy in the remainder of this chapter provides limited insights into the answers to these questions. For example, there is little indication that any permanent change is about to occur to reconcile the different views of the national interest and how these should be addressed in policy on the security of electronic information. It is more likely, given the complexity of the issues, that the narrower ones will be addressed, such as the extent of controls on information flows v. the ease of public access to Federal information intended by the Freedom of Information

Table 12.—Government Actions Affecting the Security of Information in Computer and Communications Systems

	Executive Branch	Legislative Branch	Key Reports
World War I	War Department[a]		
Post World War I	American Black Chamber[b]		
1934		Communications Act[c]	
1952	NSA created[d]		
1965		Brooks Act[e]	
1968		Omnibus Crime Control and Safe Streets Act[f]	
1976			Senate report on Federal intelligence functions[g]
1977	NBS establishes DES as U.S. standard		MITRE reports on communications security[h]
1978		Foreign Intelligence Surveillance Act[i]	
1979	Policy on protection of government communications, PD/NSC-24[j]		RAND report on computer security[k]
1980			NTIA White Paper[l]
1981	Executive Order 12333[m]		
1984	Policy on protection of government computer and communications systems, NSDD 145.[n]		
1985		House hearings on computer security policy[o]	
1986	Policy on protection of sensitive information[q] NSA decision to replace DES	HR 145, Computer Security Act[p] Computer Fraud and Abuse act[r] Electronic Communications Privacy Act[s]	
1987	Planned review of NSDD[q]	House hearings on HR 145[t]	House report on computer security[u]

[a] Responsibilities of the War Department included safeguarding classified and diplomatic messages and signals intelligence operations.

[b] H.O. Yardley, *The American Black Chamber*, Bobbs-Merrill Co., Indianapolis, 1931. As reported in David Kahn, *The Codebreakers*, pp. 360-361.

[c] The Communications Act of 1934, Section 605 (now section 705), as amended.

[d] The National Security Agency was created by a still-classified Presidential memorandum in 1952. NSA's responsibilities include safeguarding Government classified and diplomatic communications and foreign signals intelligence operation.

[e] Public Law 89-306.

[f] Title 3 of the Omnibus Crime Control and Safe Streets Act of 1968 protects the privacy of wire and oral communications and delineates conditions under which interception of wire and oral communications may be authorized.

[g] "The Evolution and Organization of the Federal Intelligency Function: A Brief Overview (1776-1975)," Supplementary Reports on Intelligence Activities, Book VI, Senate Select Committee to Study Government Operations, Report 94-755, Apr. 23, 1976.

[h] "Study of the Vulnerability of Electronic Communications Systems to Electronic Interception," Volumns 1 & 2, the MITRE Corp., January 1977; "Selected Examples of Possible Approaches to Electronic Communications Intercept Operations," the MITRE Corp., January 1977. These reports were prepared under contract to the Office of Telecommunications Policy, Executive Office of the President.

[i] Public Law 95-511 establishes standards and procedures for the use of electronic surveillance for Government intelligence collection within the United States, including wiretaps and radio interception.

[j] Presidential Directive/National Security Council-24 (PD/NSC-24), Telecommunications Protection Policy (unclassified excerpts, dated Feb. 9, 1979), Nov. 16, 1977 (classified).

[k] "Security Controls for Computer Systems," Report of the Defense Science Board, Task Force on Computer Security. Originally published as a classified document (R-609), February 1970. Republished as R-609-1 by the RAND Corp., October 1979 (unclassified).

[l] "Analysis of National Policy Options for Cryptography," National Telecommunications and Information Administration, Department of Commerce, Oct. 29, 1980.

[m] Executive Order 12333, United States Intelligence Activities, Dec. 4, 1981. The order includes a description of certain authorities of NSA for communications security safeguards.

[n] NSDD 145, Policy on Telecommunications and Automated Information System Security, Sept. 17, 1984, assigns responsibility for computer and communications security to a single executive agent, the Secretary of Defense, and a single national manager, the Director of NSA.

[o] Hearings on computer security policies, House Subcommittee on Transportation, Aviation, and Materials, Committee on Science and Technology, June 27, 1985.

[p] The Computer Security Act of 1986 (now 1987), HR 145.

[q] Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunication and Automated Systems, NTISSP No. 2, Oct. 29, 1986. This policy provides a definition of such sensitive information and notes the responsibilities of department heads for deciding when safeguards are warranted. This policy was rescinded in March 1987 by Frank Carlucci, Chairman, National Security Council, and at the same time, a review of NSDD 145 was ordered.

[r] Public Law 99-474 provides penalties for unauthorized access to certain financial records in computer systems and for trespassing on Federal computers.

[s] Public Law 99-508 amends Title 3 of the Omnibus Crime Control and Safe Streets Act of 1968. It protects against the unauthorized interception of electronic communications.

[t] Hearings on HR 145 of the House Subcommittee on Legislation and National Security, Feb. 25-26, and Mar. 17, 1987, and joint hearings of the House Subcommittee on Transportation, Aviation, and Materials, Feb. 26, 1987.

[u] House report 100-153, Parts 1 and 2, June 11, 1987, 100th Cong., 1st Sess.

Act, and the appropriate roles of NSA v. NBS in providing safeguard standards for nondefense use.

Finding an appropriate balance between these different views is not easy. Both are embodied in laws and policies, and both have strong advocates within and outside Government. Moreover, they have an existence that transcends the current debate over information security. Still, the issues raised by the debate demand attention now because of the implications of information security for the conduct of government, business, science, and our personal lives.

Two important shifts appear to be occurring, however. The first is a wider recognition of the impacts of policies on users of information security products and on providers of information services, particularly where the public does not understand or agree with the need for controls, or where impacts fall unevenly. The second major shift, one that is still being deliberated, is a reluctance by Congress to accept executive branch policies on information security when they require subordinating other important national interests. These two trends suggest that future policies for national security will have to be integrated with other interests, or alternative means found for satisfying them, such as through the technological and administrative safeguard measures noted in chapters 4 and 5.

THE EVOLUTION OF FEDERAL POLICY FOR SAFEGUARDING UNCLASSIFIED INFORMATION IN COMMUNICATIONS AND COMPUTER SYSTEMS

Executive Branch Activities in Information Security

Government policies have focused on the confidentiality of electronic communications since before World War I.[4] These policies provided the means for protecting classified defense and diplomatic messages transmitted over Government and commercial communications systems. For most of this century, U.S. policies included both communications security and signals intelligence operations against foreign governments.[5] These functions became dispersed within each of the military departments, but were consolidated with the creation of the National Security Agency (NSA) within DoD in 1952.[6]

While U.S. defense agencies have long had an interest in preventing Soviet acquisition of various militarily useful equipment produced in this country or by our allies, they have also begun of late to urge export protection of technical information that could be used for military or commercial purposes. Consequently, in some policy circles, the concept of national security, which in times past was very familiar to our understanding of "national defense and foreign policy," has taken on a broader meaning, one encompassing a wide range of economic, technical, scientific, and business information.

At the same time, two other concerns have arisen. One is over Soviet and other countries' electronic intelligence gathering in the United States. A second involves an increase in the range of potential international adversaries. No longer are they perceived as limited to military and diplomatic opponents, but include economic rivals as well as terrorists, drug traffickers, and organized crime.

From such considerations have come an increasing interest in protecting information that, although not classified, is nevertheless important or sensitive enough alone or in combination with other unclassified information to warrant special precautions. As a consequence, a new category of unclassified, but sensitive information has developed.

---

[4] For an account of early Government intelligence operations, including wiretapping, codemaking, and codebreaking, see: Supplementary Reports on Intelligence Activities, Book 6, Final Report of the Select Committee to Study Government Operations with respect to Intelligence Activities, U.S. Senate, Report No. 94-755, Apr. 23, 1976.

[5] James Bamford, *The Puzzle Palace* (New York, NY: Penguin Books, 1983), p. 206. The Army's cryptologic capability dates at least to World War 1.

[6] Ibid., p. 81. NSA was created by a top secret presidential order signed by President Harry S Truman on Oct. 24, 1952.

Computer Security

Executive branch interest in computer security began with the establishment of a task force in 1967 to recommend safeguards to protect classified information in multi-access, resource-sharing computer systems. The work of the task force, which was sponsored by DoD's Defense Advanced Research Projects Agency, resulted in a classified report issued by the Defense Science Board in 1970, a declassified version of which was published in 1979.[7]

At the same time, NSA, which was concerned about the vulnerability of the U.S. banking system, began encouraging NBS to become involved in computer security. Based on the authority of the Automatic Data Processing Equipment Act (widely known as the Brooks Act) of 1965,[8] NBS was already developing performance standards for computers used by the Federal Government. As a result, NBS and the Association of Computing Machinery cosponsored a conference in 1972 on computer security. Following the conference, NBS initiated a program in computer and communications security in 1973 based on the Brooks Act. This program led to the adoption in 1977 of the Data Encryption Standard (DES), as a national standard for cryptography. (See ch. 4.)

Since then, NBS has published dozens of Federal Information Processing Standards and guidelines, validated commercial encryption devices, participated in voluntary standards groups, assisted other civilian agencies, and, with NSA, cosponsored annual conferences on computer security. NBS also works with users and vendors in developing many of their products. Recently, the agency has contributed to the development of standards for network security as part of the "open system interconnection network."

The 1970 task force report also prompted DoD to improve the security of classified information in computer systems. Research and development undertaken by the Air Force, Defense Advanced Research Projects Agency, and other defense agencies in the early- and mid-1970s demonstrated approaches to technical problems associated with controlling shared-use computer systems.[9]

As a result of these activities, DoD launched the Computer Security Initiative in 1978, a program largely transferred to NSA in 1981, to address the department's computer security needs. The program became the National Computer Security Center (NCSC) in 1984 with the issuance of NSDD-145. NCSC develops standards and guidelines, evaluates computer hardware and software security properties, undertakes research and development, and trains users. According to NCSC literature, the center addresses the Nation's computer security problems rather than just those associated with classified information or defense agency requirements.

Many of NCSC's activities affect civilian agencies and the private sector. Among these are the development of criteria for evaluating the security of trusted computers, known as the "Orange Book."[10] NCSC, or other parts of NSA, rate commercial products based on the orange book criteria and train people in computer security, evaluate commercial DES products and other cryptographic devices,[11] design cryptographic modules for vendor manufacture, and develop secure telephone equipment. NCSC also publishes standards and guidelines for computer security and participates in voluntary standards activities with industry. (See ch. 5.)

---

[7] Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security, Office of the Secretary of Defense. Originally published as a classified document (R-609), February 1970; republished as an unclassified document (R-609-1), October 1979, by the RAND Corp., Willis Ware, editor.

[8] Public Law 89-306, Automatic Data Processing Equipment Act of 1965.

[9] J. P. Anderson, "Computer Security Technology Planning Study," ESD-TR-73-51, vol. I, AD-758 206, ESD/AFSC, October 1972.

[10] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985. See also CSC-STD-001-83, Aug. 15, 1983.

[11] Under the Commercial Communications Security Endorsement Program.

Communications Security

PD/NSC-24

Increasing concern during the mid-1970s about Soviet interception of unclassified U.S. domestic communications led to a change in executive branch policy. Presidential Directive/National Security Council-24 (PD/NSC-24) was signed by President Jimmy Carter in 1977. It expanded the authority of DoD and, in a more limited way, the Department of Commerce, for safeguarding unclassified, but sensitive communications that "would be useful to an adversary."[12] PD/NSC-24 directed Federal department heads to protect unclassified, but sensitive communications. It assigned responsibility to DoD for the security of classified communications and for unclassified, but sensitive communications related to national security. It also assigned responsibility to the Department of Commerce for raising users' awareness of the vulnerability to interception of communications systems. In addition, PD/NSC-24 charged the Defense and Commerce Departments with developing a joint proposal for a national policy on cryptography. DoD's responsibilities were carried out by NSA and Commerce's National Telecommunications and Information Administration (NTIA).

Several DoD directives were issued to implement PD/NSC-24. The first, National Communications Security Council Policy-10 (NCSC-10),[13] called for the protection of sensitive information transmitted by the Government or DoD contractors over satellite links. It was followed by NCSC-11,[14] which broadened NCSC-10 to protect all transmission systems carrying sensitive information from Government and DoD contractors. Neither NCSC-10 nor NCSC-11 included a funding mechanism, but NSA issued National Communication Security Instruction 6002 in 1984.[15] It authorized Federal agencies and Government contractors to purchase approved equipment and services to protect unclassified, but sensitive information. (See ch. 5.) For its part, NTIA conducted seminars on communications vulnerabilities for more than 1,500 Federal employees.

DoD and Commerce were not able to develop a joint proposal for a national policy on cryptography, however, because of disagreements over compromises concerning national security, trade, innovation, and First Amendment rights. Instead DoD and Commerce submitted separate proposals. Essentially, the DoD proposal called for a continuation of various Government controls on cryptography, such as on patents and the export of equipment and technical data, while Commerce proposed minimizing these controls and argued for greater sensitivity to the negative effects they have on broader national interests.[16]

The NTIA effort under PD/NSC-24 was hindered significantly by the absence of definitions of the terms "sensitive information" and "useful to a foreign adversary" that could serve as practical guides to department heads. This shortcoming is significant because the broad definition provided in NSDD-145 later had to be withdrawn due to public apprehension about its potentially wide applicability.

---

[12] Presidential Directive/National Security Council-24 (PD/NSC-24), Telecommunications Protection Policy (unclassified excerpts, dated Feb. 9, 1979), Nov. 16, 1977 (classified).

[13] National Policy for the Protection of U.S. National Security Related Information Transmitted over Satellite Systems, NCSC-10, Apr. 26, 1982. The National Communications Security Council was a predecessor organization to that established under NSDD-145.

[14] National Policy for Protection of Telecommunication Systems Handling Unclassified National Security Related Information (NCSC-11), May 3, 1982.

[15] Protection of Government Contractor Telecommunications, National Communication Security Instruction 6002 (NACSI-6002), June 1984.

[16] This assessment stems from OTA staff interviews in April 1987, with former NTIA officials involved in developing the Department of Commerce proposal for a national policy on cryptography. Also, see "White Paper: Analysis of National Policy Options for Cryptography," National Telecommunications and Information Administration, U.S. Department of Commerce, Oct. 29, 1980.

PD/NSC-24 had at least two notable effects: it pioneered an experiment by assigning some limited responsibility for safeguarding Government communications to a civilian agency —the Commerce Department—and it provided authority for NSA to protect unclassified communications. The assignment to NSA was the beginning of a trend toward consolidating and broadening responsibilities for the security of unclassified electronic information within DoD.

The joint Defense and Commerce programs, begun in 1978 under PD/NSC-24, were short-lived. They ended when NTIA's involvement was discontinued in 1982 due to reasons of general agency budget reductions. Further, PD/NSC-24 itself was superceded by NSDD-145 in 1984. Many of the activities initiated under PD/NSC-24 now come under the authority of NSDD-145.

NSDD-145

The current national charter for information security is provided by Executive Order 12333[17] and National Security Decision Directive 145 (NSDD-145). Executive Order 12333 assigns to the Secretary of Defense responsibility for making Government communications secure.

NSDD-145 is the current fundamental policy for communications and computer security. It:

- recognizes the merging of communications and computer technology and is intended to direct a coordinated approach to securing both types of systems;
- continues the emphasis on protecting unclassified, but sensitive information begun under PD/NSC-24;
- assigns responsibility for computer and communications security solely to a single executive agent, the Secretary of Defense, and a single national manager, the Director of the National Security Agency; and
- establishes a specific responsibility for major Government resources to be used to "encourage, advise, and if appropriate assist" the private sector to protect against exploitation of communications and automated information systems.

NSDD-145 states that telecommunications and automated information systems "are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other forms of hostile intelligence threat." It recognizes that exploitation can occur from terrorist groups and criminal elements, and that private or proprietary information can become targets for foreign exploitation. NSDD-145 focuses on unclassified, but sensitive electronic "Government and Government-derived information, the loss of which could adversely affect the national security interest."

The directive establishes an interagency organization that includes virtually all Federal defense, intelligence, and law enforcement, as well as some civilian agencies. The leadership of the interagency group is also responsible for the security of classified information.

The organizational structure is shown in table 13. The key points to note are:

- The Systems Security Steering Group oversees the implementation of NSDD-145. It is composed of the secretaries of State, Treasury, and Defense, the Attorney General, the director of the Office of Management and Budget, and the director of the Central Intelligence Agency, and was chaired by the President's advisor for National Security Affairs as recently as 1987.
- Working under the steering group's guidance is the National Telecommunications and Information Systems Security Committee (NTISSC), which develops operating policies and provides security guidance to Government agencies. NTISSC is composed of representatives of Government agencies and departments having principle or major missions in military, intelligence, and law enforcement, among others. It is chaired by the assistant sec-

---

[17] Executive Order 12333, United States Intelligence Activities, Dec. 4, 1981.

Table 13.—Committees Guiding the Implementation of NSDD 145

Systems Security Steering Group:

1. Secretary of State
2. Secretary of the Treasury
3. Secretary of Defense[a]
4. Attorney General
5. Director of OMB
6. Director of Central Intelligence[a]
7. Assistant to the President for National Security Affairs, chair[a]

National Telecommunications and Information Systems Security Committee:

Consists of a voting representative of each of the above, plus a representative designated by each of the following:

8. Secretary of Commerce
9. Secretary of Transportation
10. Secretary of Energy
11. Chairman, Joint Chiefs of Staff[a]
12. Administrator, GSA
13. Director, FBI
14. Director, Federal Emergency Management Agency
15. Chief of Staff, Army[a]
16. Chief of Naval Operations[a]
17. Chief of Staff, Air Force[a]
18. Commandant, Marine Corps[a]
19. Director, Defense Intelligence Agency[a]
20. Director, National Security Agency[a]
21. Manager, National Communications System[a]
22. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, chair[a]

[a] Denotes a representative closely associated with the defense/national security community.

SOURCE: Donald C. Latham, Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, testimony before the House Subcommittee on Transportation, Aviation, and Materials and Subcommittee on Science, Research, and Technology, Feb. 26, 1987. See also NSDD-145, Sept. 17, 1984.

retary of defense (for command, control, communications, and intelligence).

- The interagency group's executive agent for telecommunications and information systems security is the Secretary of Defense, who approves standards and doctrine, and reviews the security budgets of other departments and agencies.
- The national manager for telecommunications and automated information systems security is the director of NSA, who serves as the Government's focal point for cryptography, telecommunications, and automated information systems security, conducts R&D for security, and approves all standards, techniques, systems, and equipments for the security of these systems.

Critics of NSDD-145 have charged that the organization is dominated by defense and intelligence interests and that the National Security Council, as chair of the steering group, acts in a decisionmaking capacity rather than as an advisor to the President. They also charge that NSDD-145 raises a conflict by giving authority to NSA to develop standards for computer security, authority that was previously given to NBS under the Brooks Act. The conflict has caused manufacturers and business users of information security products to question which Government agency has leadership for standards development, equipment endorsement, and related functions, and raised the issues of the appropriate division of responsibility between civilian and military agencies, as well as the secrecy and absence of open accountability of NSA.

Definition of Sensitive Information

Finally, there has been considerable concern over public access to unclassified, but sensitive information (see below). One main reason was the definition of the term as information whose loss, misuse, alteration, or destruction "could adversely affect national security or other Federal interests." These national security interests were defined as:

> . . . matters that relate to the national defense or the foreign relations of the U.S. Government. Other Government interests are those related, but not limited to the wide range of Government or Government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.[18]

Shortly after this definition was issued, Diane Fountaine, director of information systems for the Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence, spoke before the Information Industry Association in New York City on November 11, 1986. This official was widely quoted as saying:

---

[18] National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Systems, NTISSP No. 2, Oct. 29, 1986.

> I don't believe that the issue is whether or not we [DoD] are going to protect information. I really believe that the issue is what information we are going to protect, both from the Federal Government, both within DoD and also within industry.[19]

The overall statement was apparently intended to assure listeners that the restrictions would apply to Soviet access to U.S. databases and not to the U.S. scientific and technical community. Nevertheless, it was generally seen as foreboding by those who fear further Federal restrictions on unclassified information.

At about the same time, two other related events were publicized that reinforced concerns for Government restrictions on unclassified information. One involved reports of a classified Air Force study on foreign access to databases in the United States and other Western countries, and what can be done to limit such access.[20] The other involved well-publicized visits to commercial database firms by representatives from the Federal Bureau of Investigation, Central Intelligence Agency, and NSA asking how controls might be placed on subscribers to their systems. These visits received considerable publicity by the news media.[21]

Policy Development in Congress

While passing legislation that provided the legal basis for some Government controls on information, Congress has also sought to protect the confidentiality of electronic communications and computer information as well as individuals' rights and privacy. The laws identified below illustrate this trend, which has been occurring simultaneously and parallel to executive branch directives aimed at national security concerns. Still other laws, not shown, protect the privacy of individuals, such as the Privacy Act and the Fair Credit Reporting Act.

The Communications Act of 1934, Section 605 (now Section 705), as amended, provides that "No person not authorized by the sender shall intercept any communications and divulge . . . the content." Notwithstanding this legislation and the 1938 Supreme Court interpretation (*Nardone* v. *United States*, 302 U.S. 379) that Section 605 prohibited all telephone wiretapping even when done by Federal Government officers, Government wiretapping continued.[22]

Title III of **The Omnibus Crime Control and Safe Streets Act of 1968** includes sections that protect the privacy of wire and oral communications, and delineate on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.[23]

The Foreign Intelligence Surveillance Act of 1978 (Public Law 95-511) establishes legal standards and procedures for the use of electronic surveillance in collecting foreign intelligence and counterintelligence within the United States. Electronic surveillance is defined to include wiretaps, radio intercepts, and other forms of surveillance.[24]

The Electronic Communications Privacy Act of 1986 (Public Law 99-508) protects against the unauthorized interception of electronic communications. It amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The Electronic Communications Privacy Act addresses three limitations in Title III protection that had developed as a result of technological changes.[25] The limitations concern the "aural acquisition" of oral communications (in contrast with the acquisition of digital communications), communications over nonwire facilities, and communications over systems other than public telephone systems.

---

[19] Draft transcript of speech by Diane Fountaine's presentation at the Information Industry Association Annual Convention, Nov. 11, 1986. Transcript provided by the Information Industry Association. See also "Pentagon Weighs Data Bank Curbs," *New York Times*, Nov. 11, 1986.

[20] Op. cit., Fountaine statement.

[21] "Pentagon Weighs Data Bank Curbs," *New York Times*, Nov. 12, 1986; "Are Data Bases A Threat to National Security?" *Business Week*, Dec. 1, 1986.

[22] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties*, OTA-CIT-293 (Washington, DC: U.S Government Printing Office, October 1985), p. 18.

[23] Ibid., pp. 18-21.

[24] Ibid., pp. 20-21.

[25] For a more thorough discussion of technological changes and the legal protections for the privacy of communications see: *Federal Government Information Technology: Electronic Surveillance and Civil Liberties*, OTA-CIT-293, op. cit., October 1985.

The Electronic Communications Privacy Act of 1986 extends legal protection in each of these areas. It prohibits unauthorized interception of video and data communications. It defines "electronic communication" to include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature." Exceptions to this include the radio portion of a cordless telephone communication, any communication made through a tone-only paging device, and any communication made through a tracking device, such as is used for electronic surveillance. The 1986 act also extends protection to communications transmitted "in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system."

Communications also are protected against intentional interception regardless of the means by which they are transmitted. But the inadvertent reception of satellite transmissions or radio communications is not penalized. The Electronic Communications Privacy Act also protects against the disclosure of stored wire and electronic communications (e.g., electronic mail records) and provides legal standards for access to the transactional records of communications providers. These extended protections address some of the vulnerabilities of communication systems identified in chapter 3.

The Computer Fraud and Abuse Act of 1986 (Public Law 99-474) provides penalties for unauthorized access to certain financial records in computer systems, including a 5-year felony provision for unauthorized access to a "Federal interest computer" with an intent to defraud. It also provides for a penalty for intentional trespassing on Federal computers. The act establishes a felony provision for malicious damage to a Federal interest computer and a misdemeanor provision for posting passwords on "pirate bulletin boards."[26]

GOVERNMENT CONTROLS ON UNCLASSIFIED INFORMATION

Controls Through Legislation

At the same time that it sought to protect individual rights and privacy from Government and other intrusions, Congress also gave the executive branch authority to limit public access to certain kinds of information, both classified and unclassified. A series of laws were enacted that gave the President and certain department and agency heads power to withhold information to protect its secrecy and to restrict access to it.

The Atomic Energy Act of 1946 (60 Stat. 755). One of the Federal Government's oldest mechanisms for controlling scientific communications, the Atomic Energy Act of 1946, had its origins in the rigid secrecy surrounding the World War II Manhattan Project and the Government monopoly on atomic energy research and development.[27] The Atomic Energy Act created the category of Restricted Data, which it defined as "all data concerning (1) design, manufacture or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy." A revised version, enacted as the Atomic Energy Act of 1954 (68 Stat. 919; 42 U.S.C. 2011-2296), permitted access and retention to some Restricted Data by private firms engaged under license in industrial applications of nuclear power, provided that they obtained the necessary security clearances and abided by the required information controls.

---

[26] Public Law 99-474, The Computer Fraud and Abuse Act of 1986, signed into law Oct. 16, 1986. Computer Crime and Security, Issue Brief, Congressional Research Service, IB85155, Mar. 10, 1987.

[27] U.S. Congress, House Committee on Government Operations, "The Government's Classification of Private Ideas," House Report 96-1540, 96th Cong., 2d sess., Dec. 22, 1980.

Without explicitly using the phrase "born classified," the Atomic Energy Act provides that Restricted Data is subject to secrecy from the moment of its creation, even though the creator may be a private individual. The Government has taken legal action against private parties, most notably *The Progressive* magazine, which was planning to publish an article (based on declassified, publicly available information) on the workings of a hydrogen bomb. The Government sought to restrain the magazine from printing the story. A court's preliminary injunction was later vacated after similar information was published in a newspaper.[28]

The act's scope was broadened in 1981 to permit the Secretary of Energy to prohibit dissemination of certain unclassified information if dissemination could reasonably be expected to have a significant adverse effect on the health and safety of the public or the national defense and security by significantly increasing the likelihood of illegal weapons production or theft, diversion, or sabotage of nuclear materials, equipment, or facilities. Declassification alone may not release certain types of information from statutory control of its dissemination.[29]

The Export Administration Act and Arms Export Control Act. Both the Export Administration Act (50 U.S.C. App. 2401-2420) and the Arms Export Control Act (22 U.S.C. 2751-2794) provide authority to control the dissemination to foreign nationals of scientific and technical data related to items requiring export licenses according to the Export Administration Regulations (EAR) or the International Traffic in Arms Regulations (ITAR). The implementing regulations are administered by the Department of Commerce, which licenses items subject to EAR, and by the Department of State, which licenses items subject to ITAR. The export of communications and computer security products and technical data are controlled through EAR and ITAR. The Defense Department plays an advisory role regarding the application of these regulations to technical data.

The term "technical data" is defined broadly to restrict the domestic dissemination of scientific and technical information to foreigners, including the presentation of papers at open scientific meetings.[30] This broad definition of "export" and the extent to which much scientific research can be (at least indirectly) related to items subject to controls have aroused much controversy during the past 7 years. The controversy pits the research and academic communities against the Departments of Commerce, State, and Defense.

Specific issues have included prepublication review clauses and other contract restraints on unclassified Government-sponsored university research, controls on foreign visitors, inquiries into and restrictions on foreign student activities (including access to supercomputer and advanced materials research), and DoD controls on the content of scientific communications at normally open professional meetings. An example of the latter was the meeting held by the Society of Photo-Optical Engineers in 1982, at which DoD forced the withdrawal of about 100 unclassified technical papers.[31]

---

[28] Harold C. Relyea: "National Security Controls and Scientific Information," CRS Issue Brief IB82083, June 17, 1986, p. 7.

[29] By contrast, uncontrolled dissemination of declassified documents—through NTIS, for example—has been criticized as being a continuing and important source of U.S. technology for the Soviet Union. See, for example: *Soviet Acquisition of Militarily Significant Western Technology: An Update*, DoD, 1985; and "Baldridge Claims U.S. Agencies Give Technology to Soviets," *Research and Development*, April 1985, p. 54.

[30] Relyea, op. cit., CRS IB82083, p. 8.

[31] See, for example: "Federal Restrictions on the Free Flow of Academic Information and Ideas," *Government Information Quarterly*, vol. 3, No. 1, 1986; Mitchel B. Wallerstein, "Scientific Communication and National Security in 1984," *Science*, vol. 224, pp. 460-466; Paul Mann, "Strictures on Non-Secret Data Concern Scientific Community," *Aviation Week and Space Technology*, Nov. 19, 1984, pp. 24-25; James K. Gordon, "Universities Resisting Potential Supercomputer Access Restrictions," *Aviation Week and Space Technology*, Aug. 26, 1985, pp. 59-62.

One of the outcomes of these controversies was the establishment of an ad hoc National Academy of Sciences Panel on Scientific Communication and National Security, chaired by Cornell University president-emeritus Dale Corson. The Corson panel report concluded that national policies of "security through secrecy" would ultimately weaken U.S. technological capabilities and recommended that contract controls be used for the (few) "gray" unclassified areas that could not reasonably be completely open.

The Invention Secrecy Act. The Invention Secrecy Act of 1951 (35 U.S.C. 181-188) provides that whenever the publication or disclosure by the grant of a patent on an invention—whether or not the Government has a property interest—might, in the opinion of the Secretary of Energy or the head of any designated defense agency (and the Department of Justice), be detrimental to national security, then that agency head can request the Commissioner of Patents and Trademarks to order that the invention be kept secret and withhold granting a patent. A patent secrecy order is issued for one year, but may be extended.

In addition to domestic patent secrecy orders, the Invention Secrecy Act provides that a license must be obtained from the Commissioner of Patents and Trademarks before filing any foreign patent application or registering any such design or model with a foreign patent office or agency for an invention made in the United States (35 U.S.C. 184).

Although the number of secrecy orders on cryptography patent inventions is small now, that was not always the case. According to a former director, NSA rescinded 62 of them in one year alone and sponsored 260 secrecy orders over a period of time.[32] It is not clear how much of a chilling effect prospective secrecy orders have on inventors.

The Defense Authorization Act of 1984. The Defense Authorization Act of 1984 provides authority to the Secretary of Defense to withhold from public disclosure certain technical data with military or space applications. The data must be in the possession or under the control of DoD and must fall within the scope of U.S. export control regulations (i.e., the data must be already subject to export controls).[33]

Executive Branch Directives and Other Restrictions

As a compromise response to the controversy concerning restraints on the communication of scientific research and to the National Academy of Science's Corson Panel Report, President Ronald Reagan issued a directive on the transfer of scientific, technical, and engineering information on September 21, 1985. Known as National Security Decision Directive 189, (NSDD-189), the directive sought to minimize controls on fundamental research and to use classified procedures where controls are needed.

Specifically, NSDD-189 states:

> . . . to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during Federally funded fundamental research in science, technology, and engineering at colleges, universities, and laboratories is classification. . . . No restriction may be placed on the conduct or reporting of Federally funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes.

NSDD-189 made Federal agencies sponsoring research responsible for determining, before the award of a research contract or grant, whether classification is appropriate and for periodically reviewing grants and contracts for potential classification.

The directive did not quell all controversy, however, because it left "applicable U.S. statutes," such as the export control laws, available as an alternative method of controlling federally sponsored, unclassified research results. Since export controls on scientific information had been a cause of the original controversy, NSDD-189 thus failed to resolve the issue.[34]

---

[32] Testimony of NSA Director, Admiral Bobby R. Inman, before the House Subcommittee on Government Information, Mar. 20, 1980. Also see "White Paper: Analysis of National Policy Options for Cryptography," National Telecommunications and Information Administration, Department of Commerce, Oct. 29, 1980.

[33] Department of Defense Authorization Act, 1984, Public Law 98-94, Sept. 24, 1983, Sec. 1217, Authority to Withhold from Public Disclosure Certain Technical Data. 10 U.S.C. 140c.

[34] See: Relyea, op. cit., CRS IB82083, pp. 12-13; and "Reagan Issues Order on Science Secrecy: Will It Be Obeyed?" *Physics Today*, November 1985, pp. 55-58.

Meanwhile, the National Aeronautics and Space Administration (NASA) limits its distribution of some unclassified scientific and technical information, including that pertaining to dual-use technologies such as the space station, satellites, experimental aircraft, or transatmospheric vehicles. Such data can be restricted from dissemination to foreigners through export control laws, particularly through ITAR, or through other means (see below), if they have significant potential domestic benefit. Some NASA officials, however, feel a need for stronger protection against Freedom of Information Act requests from citizens of foreign countries. NASA officials try to screen such requests for unclassified reports listed in the RECON database, which contains abstracts and briefs from NASA technical reports. Foreign requesters are referred to the Department of State for licensing if the material is subject to ITAR.

NASA's charter calls for the agency to disseminate information in an "appropriate" manner. This can include "early domestic dissemination" of data that is subject to limited distribution, in which case the data is made available to U.S. industry with the proviso that it not be published or disseminated abroad for a period of time. In some cases, "appropriate" dissemination may be determined by consideration of U.S. economic competitiveness as well as by national security concerns.[35]

NASA does not make the services and documents in its technical utilization program available to foreign requesters or to their domestic U.S. representatives. For many years the NASA Scientific and Technical Information Facility has screened all requests for subscription to *NASA Tech Briefs*, technical support packages, and other documentation.[36] This practice, apparently motivated by concerns for national security and/or economic competitiveness and inferred from the export control laws, resulted in the NASA "No-No" list often being cited in the controversies surrounding National Telecommunications and Information Systems Security Policy Number 2 (NTISSP No. 2)[37] and the prospect of Government controls on commercial databases.

NTISSP No. 2 was formally adopted as national policy on October 29, 1986. It defines unclassified, but sensitive information to be used in accordance with the telecommunications and automated information system security policy set out in NSDD-145. NTISSP No. 2 extended Federal concerns for safeguarding information beyond national security interests to concerns for broader national interests as described above. Federal agency and department heads were directed to identify unclassified, but sensitive information that might warrant protection in telecommunications or information processing systems, to determine in coordination with the National Security Agency (NSA) the threats to and vulnerabilities of these systems, and to implement appropriate security measures consistent with Office of Management and Budget Circulars A-123 and A-130. (See ch. 5.)

NTISSP No. 2's broad definition of unclassified, but sensitive information and its implied extension of NSDD-145 into such a wide range of public and private sector information systems caused considerable controversy and outcry, as noted earlier, particularly because of implications for controls on scientific and financial information and commercial databases[38] NTISSP No. 2 was rescinded in March, 1987.

NSA does not have statutory authority to require prepublication review of independent, nongovernment research in cryptography. Nevertheless, the agency has attempted during the past decade to control publication and research funding in cryptography, efforts that have caused controversy. In the mid- and late 1970s, NSA attempted to assume the responsibilities of the National Science Foundation for funding unclassified cryptographic research, including reviewing research proposals and results.[39]

---

[35] OTA telephone interview with G. T. McCoy, NASA Office of the General Counsel, Patent Counsel Section, Mar. 31, 1987; comments from R. F. Kempf, Associate General Counsel for Intellectual Property Law, NASA, received May 8, 1987.

[36] Walter Heiland in NASA memo, "The So-called No-No List," dated Sept. 30, 1986.

[37] Op. cit. National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, Oct. 29, 1986.

[38] "Making Waves: Poindexter Sails Into Scientific Databases," *Physics Today*, January 1987, pp. 51-52.

NSA has also requested patent secrecy orders on applications for cryptographic equipment and algorithms under authority of the Invention Secrecy Act. Controversy concerning two secrecy orders led NSA to request the American Council on Education (ACE) to form a study group on cryptography. The ACE group was assembled in 1980 and issued its report the next year. It recommended the establishment of a voluntary prepublication review arrangement between NSA and academic researchers.[40]

As a result, NSA established a voluntary process for cryptographic manuscripts, with simultaneous review by NSA officials and professional journals, and with an appeals committee. Although the merits of such a process are still subject to some debate, some participants consider that it works in a reasonably satisfactory manner. According to *Science* magazine, about 200 papers had been submitted to NSA for review by 1984. According to NSA, of that number, nine papers were challenged. Six of these were modified and three withdrawn.[41]

THE ENVIRONMENT FOR POLICY DEVELOPMENT

The Early Environment

Cryptography has long been the principal method for protecting the confidentiality of communications. Since World War I, and increasingly during the past four decades, the Federal Government has been the Nation's main source of expertise in the U.S. for developing cryptographic techniques. With rare exceptions, these developments, including cryptographic algorithms, have been kept secret, as has similar work in other nations.

Prior to the mid-1970s, there were relatively few external complications to communications policies based exclusively on national security concerns. NSA, and DoD generally, had responsibility for communications security and the private sector had little interest in cryptographic technology. The Government could protect its interest by classifying R&D, controlling patent grants and exports, and monopolizing talent in the field. Any negative effect of this secrecy and controls on private sector activities, presumably, have been relatively minor, with the possible exception of restrictions on patents and exports of cryptographic equipment and technical data.

The Changing Environment and Federal Policies

During the past decade, a number of events have changed the external environment, changes that are still taking place. The first of these has to do with shifts in Federal policy and the second concerns the changing external environment for policymaking.

Federal policy took a sharp turn in the 1970s when a nondefense agency, NBS, became involved in cryptography for the first time. The result of NBS' efforts, which NSA assisted, was adoption of the Data Encryption Standard (DES) as a national standard for cryptography, the inner workings of which were published in the open literature.

---

[39] See ch. 4. See also Tom Ferguson, "Private Locks, Public Keys and State Secrets: New Problems in Guarding Information with Cryptography," Center for Information Policy Research, Harvard University, April 1982, and "The Government's Classification of Private Ideas," House Committee on Government Operations (op. cit.).

[40] "Report to the Public Cryptography Study Group," *Academe*, vol. 67, December 1981.

[41] Mitchel B. Wallerstein, "Scientific Communications and National Security in 1984," *Science*, vol. 224, pp. 460-466.

The change in policy direction from secrecy to openness appears to have signaled increasing interest in the defense and intelligence communities in finding ways to thwart the ability of the Soviet Union and others to gain access to unclassified, unprotected U.S. communications. The policy shift is widely known to have triggered debate within NSA as to the tradeoffs between potential gains in securing communications at the expense of losses to the agency's signals intelligence mission. Debates outside of the agency questioned whether NSA, in view of its signals intelligence mission, would permit a high quality cryptographic algorithm to be published in its entirety.

Then, in the late 1970s, heightened Federal concern for foreign interception of U.S. Government and private sector communications resulted in the issuance of Presidential Directive/National Security Council 24, as noted earlier. PD/NSC-24 called for raising public awareness of the vulnerability of communications systems to interception. Thus, cryptography, the central means for safeguarding communications that are easy to intercept, was destined to play a role in the security of nondefense communications.

As these Federal policies evolved, important changes were also taking place outside the Government as private sector interests and competence in cryptography and other safeguard technologies began to grow. These changes were stimulated by the almost simultaneous invention of DES and the public-key algorithm by researchers from industry and academia.(See ch. 4.) This was followed in the late 1970s and early 1980s by private sector users recognizing new applications for these technologies. The result was a new set of stakeholders with an interest in Federal policies in this area.(See ch. 5.) In addition, business interest in cryptography became international. These events contribute to an environment that contrasts sharply with the relatively tranquil one in which earlier U.S. policies were established.

The Current and Future Environment

The current external environment continues to evolve in a number of ways, some of which are an extrapolation of the past decade. For example:

- The private sector and civilian Government agencies are increasingly interested in improved safeguards for automated information systems, particularly for computer systems and for computer-communications networks. Computer safeguards are developing rapidly using a number of technologies, only a few of which are based on cryptography.
- Business applications for cryptography are still growing both in the United States and overseas.[42] Uses include improved confidentiality of data, message authentication and verification, and user identification. These new applications often take unpredictable forms, such as streamlining routine paper transactions in automobile manufacturing and reducing inventory costs in the grocery industry.
- There is an expanding, although by no means comprehensive, technical competence in the private sector to develop cryptographic-based and other safeguard technologies.

In this setting, defense policymaking has resulted in two recent changes. First, NSA sees its current role as the focal point for all computer and communications security for the Federal Government and private industry, including the protection of unclassified, but sensitive information.[43]

Secondly, NSA changed the Federal Government's practice of openly publishing cryptographic algorithms. The agency announced in 1986 that it would not recertify DES-based products after January 1988. Previously endorsed DES products may continue to be used, in general, and DES also may continue to be used for Government electronic fund transfers.[44] In place of DES, NSA announced that it would offer a family of NSA-designed and -certified algorithms embedded in tamper-proof modules to protect unclassified information.

---

[42] Richard I. Polis, "European Needs and Attitudes Toward Information Security," unpublished paper prepared for the Fifteenth Annual Telecommunications Policy Research Conference, Airlie, VA. Sept. 27-30, 1987.

[43] NSA announcement, April 1986.

Thus, the prior Federal Government policy of providing certified, published algorithms, developed as consensual standards under NBS stewardship, has in fact shifted to NSA-provided, secret algorithms as a means of providing improved protection against the misuse of unclassified electronic information.

---

[44] Letter from NSA to OTA from Michael C. Gidos, Chief, INFOSEC Policy, COMSEC Doctrine, and Liaison Staff, dated July 23, 1986.

CURRENT CONGRESSIONAL INTEREST

The various interests, concerns, and policy trends described in this chapter provide a background for a set of policy issues reflected in proposed legislation and hearings on computer and communications security in Congress during 1986 and 1987. Issues and concerns that previously were spoken of privately now were said in public and for the record. The result may be a vehicle for resolving, at least in the short run, some of the conflicting interests and views of national security as they pertain to the security of computer and communications information.

The Computer Security Act of 1987 (HR 145) was introduced in the House of Representatives in 1987.[45] It would establish a Government-wide program to ensure the security of sensitive information in computer and communications systems. Specifically, the bill:

- assigns to NBS responsibility for assessing the vulnerability of the Federal Government's computer and communications systems, and for developing appropriate security standards and guidelines, as well as providing technical assistance to other agencies;
- requires NBS to develop guidelines for use in training Federal personnel in computer security;
- defines unclassified, but sensitive information broadly to include information, "the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under . . . the Privacy Act . . ."; and
- provides an advisory role for NSA to NBS concerning safeguard technology, but does not affect NSA's responsibilities for safeguarding classified information.

HR 145 establishes agency responsibilities for the development and standardization of safeguards to protect sensitive information against loss and unauthorized modification or disclosure, and to prevent computer-related fraud and misuse. As part of its role, NBS would develop standards and validation procedures for safeguards, provide liaison with other Government agencies and private organizations, and assist Federal agencies and the private sector in applying NBS-developed standards and guidelines. An advisory board would be established to assist NBS, which would include NSA representation.

Congressional hearings were conducted on HR 145 and NSDD 145 on February 25 and 26 and on March 17, 1987, by the Subcommittee on Legislation and National Security of the House Committee on Government Operations. Joint hearings were also held on February 26, 1987 by the Subcommittee on Science, Research, and Technology, and the Subcommittee on Transportation, Aviation, and Materials of the House Committee on Science, Space, and Technology.

The hearings were significant because they allowed representatives of important scientific, professional, and trade groups to publicly express their concerns. Witnesses at the hearings commenting on their experiences or views on NSDD-145 were generally negative or apprehensive. Their comments tended to focus on three main points:

---

[45] H.R. 145, The Computer Security Act of 1987, Jan. 6, 1987, and report 100-153, Parts 1 and 2, June 11, 1987.

1. NSA's expanding role in civilian agency and private sector computer security;
2. the "disruptive," "counterproductive" effects of NSA's restrictions on U.S. banks' use of NSA-provided cryptographic algorithms; and
3. apprehension regarding potential DoD controls on unclassified information.

Many witnesses at these hearings were concerned that, under NSDD-145, the Government would restrict access to information in public libraries, engineering and scientific publications, and Government and commercial online databases. Challenges were raised as to the authority of the Government to withhold unclassified information from the public, the effect on First Amendment protections, and potential damage to the free flow of information in society and to the principle of open government.[46]

In response, DoD officials assured the subcommittees that NSDD-145 would not extend the authority of DoD or NSA to control access to unclassified, but sensitive information, nor would it apply to information in the private sector or to Government information subject to release under the Freedom of Information Act. In commenting about the purposes of NSDD-145, these officials pointed out that the Government needs to prevent invasions of citizens' privacy, the obtaining of unfair advantage in business dealings, and avoidance of law enforcement efforts,[47] once again addressing the question of the scope of national security interests.

During the course of these hearings, the definition of unclassified, but sensitive information provided in NTISSP No. 2 was rescinded and the National Security Council initiated a review of NSDD-145 aimed at reducing or eliminating its operational role.[48] At about the same time, civilian agency participation in NTISSC was expanded.[49]

These current congressional activities are the latest attempt to grapple with the diverse issues surrounding information security policy, many of which are of long standing. Regardless of the outcome of HR 145, the fundamental issues—such as the separation of power, the role of the Government, and the boundaries between military and civilian agency responsibilities—will require reexamination to determine the appropriate balance of national interests.

---

[46] See, for example, testimony of the Information Industry Association, the Institute for Electrical and Electronic Engineers, the American Library Association, the Association of Research Libraries, the American Physics Society, David Kahn, and the American Civil Liberties Union.

[47] Op. cit., Latham testimony, Feb. 26, 1987.

[48] Letters from Frank Carlucci, Assistant to the President for National Security Affairs to Congressman Jack Brooks, Chairman, Committee on Government Operations, U.S. House of Representatives, Mar. 12 and 17, 1987; Letter from Howard H. Baker, Chief of Staff to the President, to Congressman Jack Brooks, Mar. 16, 1987.

[49] From material provided by NSA staff to OTA, Dec. 22, 1986.

Chapter 7

Federal Policy Issues and Options

CONTENTS

Page
Introduction . . . 151
The Influence of Federal Policies . . . 151
Factors Influencing Information Safeguard Developments . . . 151
The National Security Influence in Policy Formulation . . . 152
Interrelated Federal Policies and Changing Concerns . . . 152
Policy Analysis . . . 153
Important Trends for Policy . . . 153
National Values and Objectives . . . 154
Levers for Implementing Policy . . . 156
Alternative Policy Options . . . 156
Evaluation of Options . . . 158
Policy Observations . . . 160

Table

Table No. *Page*
14. Policy Options . . . 157

Chapter 7

Federal Policy Issues and Options

INTRODUCTION

Policy formulation in the area of information security is important today and will become more so in the coming decade and beyond. Its importance stems from the broad impact of electronic information on society and the potentially major applications of safeguard technology for commerce and government.

As discussed earlier in this report, applications of information safeguard technology are already being adopted to improve the efficiency, integrity, and control of business and Government automated transactions, and to improve their confidentiality as well. Much larger and more pervasive applications for commerce and society are foreseen, further stimulated by continued advances in this technology.

The Influence of Federal Policies

Federal policies can have a strong influence on the development and use of information safeguards. Policies may encourage private investment in safeguard technologies or, on the other hand, can discourage such activities. Chapters 5 and 6 provide a number of examples of policies and programs that have a combination of these effects. For example, the Government can stimulate the use of safeguards by setting technical standards, requiring specific message authentication and verification procedures for certain applications, and issuing performance guidelines and specifications.

On the other hand, secret Government designs for safeguards may result in high-quality, federally endorsed commercial safeguards, but discourage independent innovation in the private sector. Secret designs also foster private sector dependence on the Federal Government for equipment validation and certification, and the provision of replacement designs.

In the defense and intelligence communities, however, Government controls are seen as vital to U.S. signals intelligence interests. Technical and other controls on access to unclassified, but sensitive information in automated systems are being considered as a means for regulating the export of valuable information to foreign interests.

Federal policies require adjustments over time as the external environment changes. During an earlier era when protecting Government-classified communications from foreign exploitation was virtually the only objective, policies shaped exclusively by this need went unchallenged and tensions with other national objectives were nonexistent or minimal. Now, however, the objectives of Federal policy are increasingly expanding to include nondefense interests, such as the prevention of embezzlement of electronic funds transfers, the disruption of public services (e.g., air traffic control and Social Security transfer payments), and the theft of proprietary information from U.S.-owned firms by foreign competitors. At the same time, the expansion of earlier policies centered on national security and Government controls is creating tensions with other national interests. Thus, new objectives are becoming important and a different balance for Federal policy may be more appropriate.

Factors Influencing Information Safeguard Developments

How and when society fully realizes the potential benefits of information safeguard technology will be determined by a number of factors. One is the aggregate need of users. We can anticipate two effects from those needs: 1) that private sector users will increasingly set the pace in new applications of safeguard technology; and 2) that market forces will respond to user demand for new products, absent Government-imposed constraints.

A second factor concerns the net effect of Federal policies on stimulating private sector developments. Federal policies to date have helped some developments in computer and communications security technology and hindered others. (See chs. 4 and 5.)

A third influence concerns private sector innovation itself. The occurrence and rate of innovations is unpredictable. Important advances, such as public-key cryptography, have occurred without Federal encouragement. Yet, Federal policies can affect the climate for creativity by stimulating research or, alternatively, creating a chilling effect.

In this view, Federal policies have a significant, but not the sole influence on private sector developments. Nevertheless, they are particularly important because today's technology is still immature and market demand limited and, in some cases, fragile. Therefore, the policies of nations that are at the forefront of technological development and innovative applications, such as the United States, will have a major impact on the pace and direction of private sector advances in information security.

The National Security Influence in Policy Formulation

An analysis of information security issues in a report based entirely on unclassified data is hindered by a number of factors, one of which is the strong influence of classified information in shaping policy development. Neither Presidential Directive/National Security Council 24 (PD/NSC-24) nor National Security Decision Directive 145 (NSDD-145), for example, were debated openly. In fact, they were classified while being developed, although eventually unclassified versions were issued. Thus, the process of policy development, at least within the executive branch, has been a relatively closed one.

Secrecy is also an important factor in policies concerning the development of cryptography. Unlike other safeguard technologies useful in computer security, cryptography is the mainstay for providing confidentiality and integrity of information that is unprotected by physical or hardware/software security measures (as when such information is in transit on a network). Cryptography allows the United States to safeguard its classified defense and diplomatic communications. The absence of high-quality encryption in foreign communications makes possible some U.S. signals intelligence operations. Because of these defense and intelligence community interests and the general lack of nondefense interests in earlier times, public policy concerning cryptography has tended to be shaped and controlled by the Department of Defense (DoD).

Until recently, policy directions based exclusively on national security concerns adequately served the Nation's needs, with little visible impact on the rest of society. That situation is changing, spurred in large part by new opportunities and challenges created by technological change, continued pressure to improve business and government operations, and the emerging internationalization of applications of this underpinning technology. This changing environment also is likely to bring further challenges to policymakers as the needs of society continue to change both in the United States and abroad.

Interrelated Federal Policies and Changing Concerns

National security interests clearly have an important and continuing place in Federal information security policies. The prospect of worldwide use of high-quality information security safeguards threatens U.S. signals intelligence operations, as does the dissemination abroad of critical technical data on information security. As technology continues to advance and as safeguards for computers and communications systems come into wider use worldwide, the effectiveness of U.S. signals intelligence may become more limited and its priority lowered among national objectives.

Another policy involves control of access by foreign governments to commercial databases in the United States that contain unclassified, but sensitive information. On-line databases allow rapid access and sorting through a wealth of information. Defense and intelligence agencies seek to prevent foreign intelligence agencies or businesses from acquiring valuable technical data that can help other countries compete with the United States militarily or economically.

Government concerns about communications and computer security, signals intelligence, and controls on foreign access to unclassified information change with time. PD/NSC-24, for example, elevated attention about the vulnerability to misuse of communications systems to Federal policy status. Now, there are a number of DoD programs, some of which are classified, to reduce those vulnerabilities. Similarly, computer security was just being identified as an area warranting Federal concern in the early 1970s. Today, substantial resources are being applied to bolster computer security. Now, concern is extending to encompass access to Government databases, such as the Defense Technical Information Center and the National Technical Information Service.

Still another change is foreseeable. For example, the proliferation of information security technology could further broaden the scope of national security concerns. Within a decade, good quality, inexpensive, easy-to-use computer and communications safeguards may be used worldwide for many applications. That could shift attention away from the central national security issues of today, possibly toward countering the use of secret transactions for conducting illegal or subversive business.

Almost at the same time that these changes in Federal concerns have been taking place, the trend in private sector users' needs for information security can now be seen as overlapping some of the Government's applications requiring message authentication, user verification, auditing of transactions, confirmation of authorizations, and confidentiality.

POLICY ANALYSIS

The preceding sections and chapters raise questions as to the appropriate overall objectives of Federal policies, the direction in which current policies may lead, and whether or not other alternatives might better serve the Nation's interests. Based on the needs of the different stakeholders, e.g., businesses, scientific organizations, and civil, defense, and intelligence agencies, it is clear that each would provide a considerably different perspective to an analysis of policy options.

Important Trends for Policy

Chapter 6 described some of the Government efforts during the past few decades to solve particular problems through controls on unclassified information. In recent years, Government efforts have included restrictions, for example, on the dissemination of unclassified technical reports from the National Aeronautics and Space Administration and potential restrictions on access to Government information of the National Technical Information Service and the Defense Technical Information Center, as well as access to information in commercial database services. Thus, there has been a tendency in Federal policy toward greater control of selected information and, recently, of access to information in certain types of systems. Some of these policies have not recognized the needs of the public.

Because computers, information systems, and communications networks are changing so rapidly, policies based only on current needs are likely to become outdated quickly. Policies are needed that are flexible and anticipate the changing needs of industry and society. The factors discussed below are among those that are changing. They will significantly influence future policy deliberations, either because of changes in the policy environment or because of the public's attitude about Federal policies that affect business operations and the free flow of information. Each provides insights into future directions for policy.

- Although some important improvements are foreseeable in the confidentiality of public communications systems, these are likely to be uneven. Many segments of these systems will remain vulnerable to exploitation by those with appropriate resources.

  To the extent that DOD programs depend on encouraging businesses to pay independently for reducing the vulnerabilities of their communications against Soviet or other foreign government interception, failure is likely since business profits are not perceived to be affected. There are strong indications, however, that some nondefense users will have business reasons to protect the integrity of certain of their information in computer and communications systems and the confidentiality of selected communications. Both interests can be served with cryptographic-based safeguards.
- A broad range of techniques for safeguarding unclassified information in computer systems and networks are available or are being developed. Private sector capabilities to develop these safeguards to meet their own needs are significant and expanding.
- Academic researchers and businesses have begun to demonstrate a level of expertise in developing certain types of cryptographic-based safeguards (e.g., the Data Encryption Standard and two-key systems). Further developments in this field are unpredictable. However, based on recent experience, Federal support for private innovation through unclassified research could yield promising results. Any additional major advances may also result in still more valuable new applications.

  These trends highlight a serious dilemma for Government policymakers: How to maintain effective signals intelligence while simultaneously encouraging the development and use of more secure systems for communications and computer systems. For example, encouraging unfettered private sector innovation in cryptography increases the chance of major technological advances that benefit commerce and society. But perhaps another country will use the same technology to protect its own electronic information from U.S. intelligence operations. On the other hand, if the National Security Agency (NSA) provides nondefense users with safeguard technology, the foreign interception and access threat may be reduced earlier, but the ready availability of "adequate" solutions from NSA may act as a disincentive for the private sector to develop solutions better tailored to its unique requirements.
- Although the current trends are not yet altogether clear, there are indications that businesses have diverse and specialized needs for cryptographic-based systems and other safeguards for a variety of nondefense applications.

  Almost certainly, no Federal agency will be able to satisfy the diverse needs of many of these users with Government-designed systems, especially if significant constraints must be placed on users.

  Private sector capabilities for developing computer and communications safeguards can meet most of the demand of Government agencies and other users. For the procurement of other commercial products, the typical practice among Federal agencies would be to provide their specific performance requirements and to purchase competitively. The arguments favoring a central role for DOD/NSA in carrying out these responsibilities are becoming less convincing, although there is a clearer need for NSA technical assistance in selected areas, such as cryptanalysis and equipment evaluation.
- Flexible Federal policies with minimal restraints are likely to have a better chance of success than others. The banking industry's experience with NSA's planned restrictions indicates that Government-pro-

vided safeguards, with rigid restraints associated with their use, are not likely to satisfy the needs of business users. (See ch. 5.)

- There is international demand for improved safeguards and foreign capabilities for developing them. (See ch. 5.)[1]
- DoD efforts to restrain or monitor foreign access to commercial on-line databases have already raised public concerns. (See ch. 6.) Further, these services are becoming a significant industry in the United States and a source of U.S. exports.[2]

  Government efforts to control access to commercial databases are likely to continue to be resisted by this rapidly growing, competitive industry.

Today, NSA appears to be attempting to retain as much control or influence as is practical in these matters. The controls are exercised mainly through authority provided under NSDD-145 and various NSA programs, including those that stimulate the availability of commercial safeguard products. Yet, the above trends suggest that Federal policies concerning the development and use of safeguard technology, and access to unclassified, but sensitive information in commercial databases, will have to be carefully aligned with changing and more intensive domestic and international business interests and with congressional and other institutions.

Some businesses are unaffected by DoD initiatives, such as those that improve the confidentiality of common carrier communications systems or that require Government-reimbursed voice protection equipment to be used by defense contractors when discussing unclassified, but sensitive information by telephone. Still other businesses are likely to support Government initiatives that enhance their operational needs, such as Federal endorsement of data encryption algorithms and certification of commercial safeguard equipment. But others are likely to oppose any Federal policies that detract from trade, innovation, open science, and civil liberties.

Finally, there are questions raised about which branch of Government should make policy on information security. Both the executive and the legislative branches have adopted policies that show few signs of coordination. The executive branch has been most active in recent years, notably with NSDD-145, and the defense and intelligence communities, specifically NSA, have been the principal implementers. Executive branch policies have been based primarily on national security considerations.

National Values and Objectives

Because there are important stakes at risk for the Nation in formulating policy for safeguarding information, Congress has to carefully consider what the Government's broad goals are that these policies seek to protect or encourage. Although there are often strong differences of opinion on the merits of specific Federal policies, there seems to be broad agreement on the types of goals that such policies might aim to achieve. Some of these goals are to:

- foster the ability of the private sector to meet the evolving needs of businesses and civil agencies for safeguard technology,
- minimize risks to U.S. signals intelligence from private sector developments, and
- clarify the roles of Federal agencies concerning unclassified information and the development and use of technology to protect it.

At the same time, achievement of the following, more general goals may also be desirable:

- promote competition, innovation, and trade;
- separate, where practical, defense and in-

---

[1] Richard I. Polis, "European Needs and Attitudes Toward Information Security" (unpublished), Telecommunications Policy and Research Conference, Airlie, VA, Sept. 30, 1987.

[2] These companies had revenues of $3.65 billion in 1984. Christopher Burns and Patricia Martin, "The Economics of Information," 1985, OTA contractor report No. 433-9520.

The industry had 486 companies by 1986. The number of database producers worldwide increased from 221 in 1979 to 1,500 in 1986, while the number of databases increased from 400 to 3,200 during that same period. OTA staff interview with Kenneth Allen, Information Industry Association, February 1987.

telligence agencies' responsibilities from those of the private sector and civilian agencies;

- retain a free flow of information and an open society, while encouraging privacy; and
- minimize or reduce the tensions between Federal policies and private sector activities.

Levers for Implementing Policy

A number of incentives and constraints can be used to implement policies regarding safeguard technologies. These include programs to certify vendors' equipment, transfer technology, standardize designs, procure devices, and encourage the development and use of improved safeguards. Controls on exports and patents are clear examples of constraints. The funding of research by the Government can be either a constraint (e.g., by keeping the results classified) or an incentive.

Depending on how some of these levers are actually used, they could simultaneously promote and restrain private sector activities. Current Government practices in transferring cryptographic technology to the private sector appear to accomplish both. They also illustrate how policy levers can be used. For example, providing a few manufacturers with high-quality, inexpensive, tamper-proof, Government-certified cryptographic devices whose design is secret may meet the immediate needs of private sector users and vendors for certified systems. Simultaneously, national security objectives are served by encouraging the use of improved safeguards. In addition, the Federal Government can control the export of these products, in part because the underlying technology is produced by a limited number of U.S. companies for NSA. At the same time, however, this approach discourages further private sector innovation since it is unlikely that many users will want or that manufacturers will produce competing products that lack NSA certification and have limited demand.

Also, some policies may encourage continued private sector dependence on the Federal Government while others are more likely to lead toward an independent technical competence in the private sector for meeting its own needs. These effects are treated in more detail in the subsequent section that evaluates alternative policy options.

The focus of decisionmaking, however, is on the respective roles of NBS and NSA, and implementing policy around these roles.

Alternative Policy Options

Several options exist for national policy. They can be distinguished mainly by the degree of centralization within the Federal Government, the level of involvement in or control of private sector activities exercised by the Government, the separation of defense and nondefense interests, the importance of national security, and the flexibility of the private sector in developing information technology safeguards to meet its needs. Table 14 illustrates the options in their main division of responsibilities between the National Bureau of Standards (NBS) and NSA.

Option 1: Centralize Federal activities relating to safeguarding unclassified information in Government electronic systems under the National Security Agency.

Option 2: Continue the current practice of de facto NSA leadership for communications and computer security, with support from the National Bureau of Standards.

Option 3: Separate the responsibilities of NSA and NBS for safeguard development along the lines of defense and nondefense requirements.

In Option 3, additional choices can be made.

A: Provide Federal support to specify, develop, and certify safeguards for businesses and civilian Government agencies. NBS would be the focal point for all safeguard standards for unclassified information. This option most closely resembles HR 145.

Table 14.—Policy Options

Responsibilities for developing standards	Option 1	Option 2	Option 3	Option 3A	Option 3B
	Centralize under NSA	Continue current practice	Separate defense and nondefense	Support private standards development	Market forces for unclassified needs
All classified	NSA	NSA	NSA	NSA	NSA
Unclassified Communications:					
Defense	NSA	NSA	NSA	NBS	NBS
Nondefense	NSA	NSA	NBS[a]	NBS[a]	NBS[a]
Computer:					
Defense	NSA	NSA	NSA	NBS	NBS
Nondefense	NSA	NSA	NBS[b]	NBS[b]	NBS[b]
Key distinctions	Centralization, NSA leadership	NSA defacto leadership	Mixed technical leadership	Commonality with nongovernment safeguards	Commonality with nongovernment safeguards Private sector leadership

[a] Refers to NBS's communications security standards responsibilities affiliated with computer security

[b] Refers to NBS's standards responsibilities under the Brooks Act (Public Law 89-306)

SOURCE: Office of Technology Assessment, 1987

B: Allow free market forces to develop safeguards for nondefense needs, with NBS acting as the focal point for Government needs for safeguards for unclassified information. NSA specifies the requirements of DoD and defense contractors and provides technical advice for other users.

The discussion of these policy options assumes that NSA would retain responsibility for matters relating to classified information in computer and communications systems under all options and that complementary NBS and NSA activities would be coordinated as necessary.

Options 1 and 3 would clarify the present confusion concerning the roles of NSA and NBS. Option 1 would provide one focal point in the Federal Government for efforts to develop safeguard technology for unclassified information in Government systems. This option would make use of NSA's technical expertise in cryptology and would concentrate the focus of U.S. policy toward national security objectives. The role of NBS in safeguard development would either be terminated or reduced to those civilian agency requirements that support NSA's role.

Option 2 would continue the current conflicting authorities assigned to NBS and NSA. It would also continue the current practice of NSA having de facto leadership in developing communications and computer security standards for the Nation, including increasing dominance over the development of cryptography. NBS would retain its current modest role in developing occasional, consensual technical guidelines and standards for civilian agency use.

Option 3 would assign to NBS responsibility for developing safeguards for all Government agencies' needs other than those specifically assigned to NSA. NSA would provide technical assistance to NBS, as needed. Under this option, NSA would be responsible for only those safeguard standards and developments required exclusively by defense agencies.

Option 3A would look to a nongovernment group or organization to take a lead role in developing consensual guidelines and standards for safeguarding unclassified information in private sector and civilian agency systems. Both NBS and NSA would actively support these private sector activities. NBS would serve as the focal point for civilian and defense agency standards for safeguarding unclassified information. As in Option 3, NSA would be responsible for providing advice to the nongovernment standards group.

Option 3B is similar to Option 3A, except that the Federal role would be diminished further. It would abandon Federal responsibilities for developing safeguards for unclassified information and, instead, would look to the market place to meet both private sector and civilian agency requirements. NBS would serve as the Government focal point for the needs of Government agencies for safeguards for unclassified information.

Evaluation of Options

The national values and objectives described earlier provide a useful starting point for comparing the policy options. It is apparent that:

> The ability of the private sector to meet its own needs is fostered as the Government increasingly allows the marketplace to satisfy agencies' needs. In computer security, where industry and the private sector have historically led, NSA's trusted computer security program has benefited from significant manufacturer input. In cryptography, the commercial communication security endorsement program has limited the scope of manufacturer innovation of encryption algorithms, reflecting the historical NSA domination of this technology. In the area of network protocols, the interface between computer security and cryptography, there has been significant "give and take" between NSA and the private sector parties directly involved in the development of standards.

On the other hand, U.S. signals intelligence capabilities would be better protected if control of private sector developments in (cryptography-based) safeguards are centralized under NSA. In the extreme case of relatively unfettered free market forces, there is a risk that signals intelligence will suffer as foreign intelligence targets benefit from safeguard products or designs developed by U.S. industry. Other factors that will affect the transfer of technology abroad include the effectiveness of U.S. export control regulations and the availability of comparable technology from foreign sources.

The current situation, which has produced considerable controversy and confusion, is essentially Option 2. Almost any option would represent an improvement in clarifying the roles of NBS and NSA. This is true whether responsibilities are centralized in one agency or divided according to divisions such as classified and unclassified information, defense and nondefense, or almost any other scheme.

Diminishing NSA's role is likely to reduce tensions between Federal policies and private sector activities in safeguard development and use. Similarly, such tensions are likely to decline as defense and intelligence interests are separated from nondefense interests.

Each of these options have other advantages and disadvantages that distinguish them. None offers a completely favorable assessment based on the objectives against which they are being evaluated. For example:

Option 1:

Pros: The key advantage that distinguishes Option 1, in addition to clarifying the responsibility of the National Security Agency, is the ability to maximize NSA's control over private sector activity in safeguard development, particularly those based on cryptography. That will allow it to minimize the risks to U.S. signals intelligence from independent private sector developments. Option 1 would be preferred if signals intelligence were the only or even the predominant policy consideration.

Cons: The main disadvantages are the likely affects of blurring defense and intelligence and civilian interests, and raising tensions due to differences in needs. Option 1 would probably have a stultifying effect on private sector innovation. The latter problem is most likely to occur in cases where new developments of value to society are detrimental to intelligence operations. The absence of a Federal standard for public-key cryptography, in spite of its obvious need, is an example of the effect of such a conflict.

Option 2:

Pros: This option retains most of the advantages of Option 1 while retaining a civilian agency to interact with private sector users, vendors, and standards organizations. In this role, NBS would maintain an awareness and perhaps advocacy of the needs of civilian users.

Cons: Perhaps the most prominent shortcoming is the lack of clarity between the roles of NBS and NSA concerning information security. In the current situation, NBS has statutory responsibility for the development of computer security standards and for serving as the Government's representative in technical standards organizations. At the same time, NSDD-145 has assigned similar responsibilities to NSA, which is charged with reviewing and approving all standards, techniques, systems, and equipment for telecommunications and automated information systems security. This option also suffers from the problems of Option 1.

Option 3:

Pros: The division of responsibilities clarifies the roles of NBS and NSA, and provides for separation between defense and nondefense needs. This option also affords an opportunity to consolidate the Government's nondefense needs with comparable needs of the private sector and to reduce tensions between defense and intelligence interests and those of the private sector.

Cons: The main shortcoming of this option concerns a lessening of NSA control of private sector innovation and its potential for damage to U.S. signals intelligence capabilities. This option also risks diluting a market that is already fragile by encouraging the adoption of different standards for defense and nondefense applications.

Option 3A:

Pros: Option 3A also would promote competition and private sector competence to meet its own needs and reduce tensions through increased Government dependence on and alignment with industry standards.

Cons: The main shortcoming, once again, concerns the potential damage to U.S. signals intelligence capabilities.

Option 3B:

Pros: The advantages are similar to those of Option 3A, but Option 3B further frees market forces and makes the Government dependent on the private sector rather than the other way around.

Cons: As in Option 3A, the main shortcoming is in potential damage to U.S. signals intelligence operations.

There are other factors for Congress to consider in evaluating the options. These include the resources required to carry out agency responsibilities under the various options, the need to carry out extensive coordination with commercial users and others in the development of standards, the ability to engender the trust of users, vendors, scientists, and others, and the ability to carry out needed research to benefit users generally.

It should also be recognized that NSA's technical expertise will be an important part of any of the options, e.g., evaluating safeguard techniques and equipments, especially those employing cryptographic methods.

As a practical matter, the resources available to NBS and NSA have not been comparable. NBS's budget for computer-related security standards has been about $10 million or less during recent years, and a staff of about 10 professionals, while NSA's National Computer Security Center alone employs some 300 people. (NSA's budget is classified.) For options in which NBS or NSA have a significant role in standards development, their efforts need to be coordinated with the needs and activities of the private sector. Although this study has not attempted to estimate the resource requirements under any of the options, some options would require changes in the funding levels of either or both NBS and NSA. In addition, it can be anticipated that any significant increase in responsibilities for the development of information safeguard technology will suffer from start-up problems, such as maintaining a high level of staff expertise, as has been the experience at NSA's National Computer Security Center.

There are a number of assumptions implicit in some of the options. One is that public acceptance of NBS standards would be based on the open scrutiny and consensual decisions that usually accompany the workings of civilian agencies. This assumption may not apply to NSA in a comparable standards-setting role given the secretive way the agency normally operates and its unilateral decision to replace DES with a secretly developed algorithm.

None of the options make allowance for conducting research. Yet, OTA's analysis indicates that society's evolving information needs depend on continuing innovations in safeguard technology. Based on observations of the rapid acceptance of DES and public key cryptography for business applications, it seems clear that there are ready applications for innovations but a limited supply of them. For now, NSA is the main source of innovation in the Federal Government. However, its signals intelligence mission is likely to prevent the dissemination abroad of U.S. innovations. Because of this constraint, innovations generated by NSA may not be made available to the public at all.

Generally, there has been little motivation for industry to sponsor long-term research from which it cannot benefit on a proprietary basis. However, the quality of proprietary cryptography tends to be suspect by some U.S. critics.[3] In this situation, the Government may decide to undertake research into selected safeguard technologies. Research into cryptographic technology is likely to raise concerns for national security if undertaken openly by NBS and concerns about public trust if undertaken secretly by NSA.

There is also the practical question of how effective restrictions imposed by the United States on its citizens might be[4] if foreign innovations, publications, and product manufacture and export are not subject to comparable restraints.

Policy Observations

There are no options for Federal policy that clearly and simultaneously foster all national goals without harming some. The alternatives differ mainly in which Government agency leads in the development of safeguard technology, the level of Federal encouragement or control of private sector innovation, and in flexibility to adjust to changing needs of businesses and society.

Three main observations result from OTA's analysis:

1. None of the policy options simultaneously satisfy all objectives.
2. Excessive accommodation of either business or defense and intelligence concerns could damage overall U.S. interests.
3. A process for weighing competing national interests is needed. Centering policymaking in the Department of Defense alone, and in particular NSA, would make that difficult.

---

[3] There are, however, indications that many Western European businesses find proprietary cryptography acceptable, according to consultant Cipher Deavours. OTA staff communications, May 1987.

[4] Richard I. Polis, "European Needs and Attitudes Toward Information Security" (unpublished), Telecommunications Policy and Research Conference, Airlie, VA, Sept. 30, 1987.

Appendixes

Appendix A

Requesting Letters

MAJORITY MEMBERS
JACK BROOKS, TEXAS, CHAIRMAN
DON FUQUA, FLORIDA
JOHN CONYERS, JR., MICHIGAN
CARDISS COLLINS, ILLINOIS
GLENN ENGLISH, OKLAHOMA
HENRY A. WAXMAN, CALIFORNIA
TED WEISS, NEW YORK
MIKE SYNAR, OKLAHOMA
STEPHEN L. NEAL, NORTH CAROLINA
DOUG BARNARD, JR., GEORGIA
BARNEY FRANK, MASSACHUSETTS
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
BARBARA BOXER, CALIFORNIA
SANDER M. LEVIN, MICHIGAN
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
JOHN M. SPRATT, JR., SOUTH CAROLINA
JOE KOLTER, PENNSYLVANIA
BEN ERDREICH, ALABAMA
GERALD D. KLECZKA, WISCONSIN
ALBERT G. BUSTAMANTE, TEXAS
MATTHEW G. MARTINEZ, CALIFORNIA

NINETY-NINTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON GOVERNMENT OPERATIONS
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515

MINORITY MEMBERS
FRANK HORTON, NEW YORK
THOMAS N. KINDNESS, OHIO
ROBERT S. WALKER, PENNSYLVANIA
WILLIAM F. CLINGER, JR., PENNSYLVANIA
ALFRED A. (AL) McCANDLESS, CALIFORNIA
LARRY E. CRAIG, IDAHO
HOWARD C. NIELSON, UTAH
JIM SAXTON, NEW JERSEY
PATRICK L. SWINDALL, GEORGIA
THOMAS D. (TOM) DELAY, TEXAS
DAVID S. MONSON, UTAH
JOSEPH J. DIOGUARDI, NEW YORK
JOHN G. ROWLAND, CONNECTICUT
RICHARD K. ARMEY, TEXAS
JIM LIGHTFOOT, IOWA
JOHN R. MILLER, WASHINGTON

MAJORITY—225-5051
MINORITY—225-5074

April 23, 1985

Dr. John H. Gibbons
Director
Office of Technology Assessment
U.S. Congress
Washington, D.C. 20510

Dear Dr. Gibbons:

The Committee on Government Operations is concerned about the potential for abuse of the telecommunication and related information systems used by the Federal Government. Despite the existence of laws requiring court orders to tap and/or tape telephone communications, there appear to be growing capabilities for surveillance of Federal phone calls and data transmissions, posing both security as well as individual privacy problems. A preliminary investigation indicates that presently there are no laws or regulations that adequately guide the proper use of this information and none that specifically prohibit the abuse of much of this information. Indeed, it is apparent that little has been done to determine the overall capacity for abuse of these communications systems or to develop methods of stopping such abuse.

A number of changes are occurring in the Federal telecommunication and other information systems that may be further contributing to this problem. First, the fundamental technology of telecommunications is changing, as are the ways in which information systems are being used and managed. Second, the number and types of applications of computer and communications technologies are increasing at a rapid rate, many of which have few safeguards against abuse. Finally, deregulation of the telecommunications services industry has shifted responsibility for the operating portions of the communications system from the telephone companies to the Federal agencies.

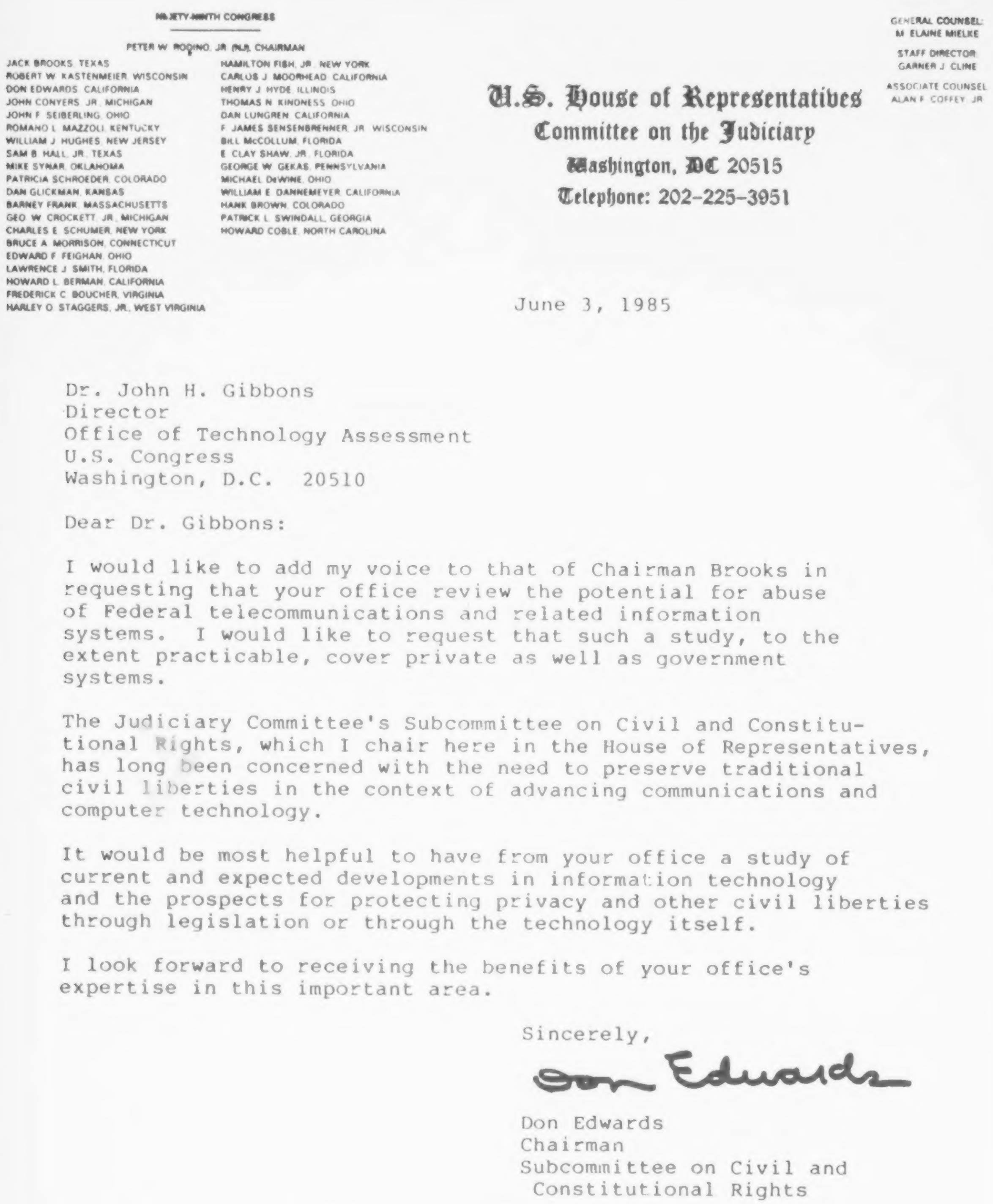
As we all know, it has been possible for decades to record telephone conversations surreptitiously. Today's technology, however, makes possible data collection and monitoring with an ease and on a scale never before realized. Tracing incoming calls; automatically recording the numbers, times, and durations of all incoming and outgoing calls; and recording prearranged conference calls are now features of many telephone systems. Other information systems used by the Federal Government, such as personal computer work stations as well as mainframes and centralized computer service systems, provide even more avenues for surreptitious data collection.

Although modern information technology is an essential ingredient in today's environment, its misuse would pose grave threats to our individual freedoms. As a result, I request that OTA undertake a review to determine the potential for abuse of Federal telecommunication and related information systems, considering both current and expected future technology, and weigh the prospects for limiting such abuses through technology and/or legislation. I appreciate your prompt attention to this request.

Sincerely,

Jack Brooks

JACK BROOKS
Chairman



NINETY-NINTH CONGRESS

PETER W. RODINO, JR. (N.J.), CHAIRMAN

JACK BROOKS, TEXAS
ROBERT W. KASTENMEIER, WISCONSIN
DON EDWARDS, CALIFORNIA
JOHN CONYERS, JR., MICHIGAN
JOHN F. SEIBERLING, OHIO
ROMANO L. MAZZOLI, KENTUCKY
WILLIAM J. HUGHES, NEW JERSEY
SAM B. HALL, JR., TEXAS
MIKE SYNAR, OKLAHOMA
PATRICIA SCHROEDER, COLORADO
DAN GLICKMAN, KANSAS
BARNEY FRANK, MASSACHUSETTS
GEO. W. CROCKETT, JR., MICHIGAN
CHARLES E. SCHUMER, NEW YORK
BRUCE A. MORRISON, CONNECTICUT
EDWARD F. FEIGHAN, OHIO
LAWRENCE J. SMITH, FLORIDA
HOWARD L. BERMAN, CALIFORNIA
FREDERICK C. BOUCHER, VIRGINIA
HARLEY O. STAGGERS, JR., WEST VIRGINIA

HAMILTON FISH, JR., NEW YORK
CARLOS J. MOORHEAD, CALIFORNIA
HENRY J. HYDE, ILLINOIS
THOMAS N. KINDNESS, OHIO
DAN LUNGREN, CALIFORNIA
F. JAMES SENSENBRENNER, JR., WISCONSIN
BILL McCOLLUM, FLORIDA
E. CLAY SHAW, JR., FLORIDA
GEORGE W. GEKAS, PENNSYLVANIA
MICHAEL DeWINE, OHIO
WILLIAM E. DANNEMEYER, CALIFORNIA
HANK BROWN, COLORADO
PATRICK L. SWINDALL, GEORGIA
HOWARD COBLE, NORTH CAROLINA

U.S. House of Representatives
Committee on the Judiciary
Washington, DC 20515
Telephone: 202-225-3951

GENERAL COUNSEL:
M. ELAINE MIELKE

STAFF DIRECTOR:
GARNER J. CLINE

ASSOCIATE COUNSEL
ALAN F. COFFEY, JR.

June 3, 1985

Dr. John H. Gibbons
Director
Office of Technology Assessment
U.S. Congress
Washington, D.C. 20510

Dear Dr. Gibbons:

I would like to add my voice to that of Chairman Brooks in requesting that your office review the potential for abuse of Federal telecommunications and related information systems. I would like to request that such a study, to the extent practicable, cover private as well as government systems.

The Judiciary Committee's Subcommittee on Civil and Constitutional Rights, which I chair here in the House of Representatives, has long been concerned with the need to preserve traditional civil liberties in the context of advancing communications and computer technology.

It would be most helpful to have from your office a study of current and expected developments in information technology and the prospects for protecting privacy and other civil liberties through legislation or through the technology itself.

I look forward to receiving the benefits of your office's expertise in this important area.

Sincerely,

Don Edwards

Don Edwards
Chairman
Subcommittee on Civil and
Constitutional Rights

Appendix B

National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems

National Telecommunications and
Information Systems Security Policy
NTISSP No. 2, Oct. 29, 1986

SSSG
SYSTEMS
SECURITY
STEERING
GROUP

CHAIRMAN

FOREWORD

NSDD-145, "National Policy on Telecommunications and Automated Information Systems Security," signed by the President on 17 September 1984, in part provides policy and direction for systems protection and safeguards for telecommunications and automated information systems that process or communicate sensitive but unclassified information. The NSDD-145 Systems Security Steering Group has established that sensitive, but unclassified information that could adversely affect national security or other Federal Government interests shall have system protection and safeguards; however, the determination of what is sensitive, but unclassified information is a responsibility of Agency heads. Executive Order 12356 prescribes requirements for classifying, declassifying, and safeguarding national security information.

This policy and the principles and procedures contained in Office of Management and Budget (OMB) Circulars Nos. A-123 and A-130, "Management of Federal Information Resources," are complementary.

John M. Poindexter

NATIONAL POLICY
ON
PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

SECTION I - POLICY

Federal Departments and Agencies shall ensure that telecommunications and automated information systems handling sensitive, but unclassified information will protect such information to the level of risk and the magnitude of loss or harm that could result from disclosure, loss, misuse, alteration, or destruction.

SECTION II - DEFINITION

Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

SECTION III - APPLICABILITY

This policy applies to all Federal Executive Branch Departments and Agencies, and entities, including their contractors, which electronically transfer, store, process, or communicate sensitive, but unclassified information.

SECTION IV - RESPONSIBILITIES

This policy assigns to the heads of Federal Government Departments and Agencies the responsibility to determine what information is sensitive, but unclassified and to provide systems protection of such information which is electronically communicated, transferred, processed, or stored on telecommunications and automated information systems. The Director of Central Intelligence shall, in addition, be responsible for identifying sensitive, but unclassified information bearing on intelligence sources and methods and for establishing the system security handling procedures and the protection required for such information.

Federal Government Department and Agency heads shall:

a. Determine which of their department's or agency's information is sensitive, but unclassified and may warrant protection as sensitive during communications or processing via telecommunications or automated information systems. This determination should be based on the department's or agency's responsibilities, policies, and experience, and those requirements imposed by Federal statutes, as well as National Manager guidance on areas that potential adversaries have targeted;

b. Identify the systems which electronically process, store, transfer, or communicate sensitive, unclassified information requiring protection;

c. Determine, in coordination with the National Manager, as appropriate, the threat to and the vulnerability of those identified systems and;

d. Develop, fund and implement telecommunications and automated information security to the extent consistent with their mission responsibilities and in coordination with the National Manager, as appropriate, to satisfy their security or protection requirements.

e. Ensure implementation of telecommunications and automated information systems security consistent with the procedures and safeguards set forth in OMB Circular A-123 and A-130.

The National Manager shall, when requested, assist Federal Government Departments and Agencies to assess the threat to and vulnerability of targeted systems, to identify and document their telecommunications and automated information systems protection needs, and to develop the necessary security architectures.

Appendix C

The Data Encryption Standard

Background on Encryption

The algorithms currently in use to encrypt (or encipher) messages and data are based on sophisticated mathematics and are usually implemented using computers or dedicated microprocessors. Nevertheless, their underlying objective is quite simple and can be traced back to antiquity:[1] to transform a message (or data) into a form that cannot be understood by anyone who does not possess special knowledge—the "key"—that unlocks the cipher and reveals the message.

Encryption takes a plaintext message and transforms it into a ciphertext (or encrypted) message using an encryption procedure and an encryption key. Thus, if P is the plaintext, E is the encryption procedure, and K_e is the encryption key, then the ciphertext, C, can be expressed mathematically as:

$$C = E(K_e, P).$$

The inverse process, decryption, given by D, transforms the ciphertext back into plaintext using the decryption key, K_d:

$$P = D(K_d, C).$$

In many encryption algorithms, the encryption and decryption keys are identical ($K_d = K_e$) and can be represented simply by K.[2] The algorithm that is used in the Data Encryption Standard (DES) uses one key, K, which is called a "private key" because the key is kept secret to ensure that outsiders cannot use it to read enciphered messages.[3]

The strength of an encryption algorithm (or cipher) can be measured by its "work factor"—the amount of effort (number of steps and time) required to "break" the cipher and read any encrypted message without the key. An algorithm's strength can be described in terms of the kinds of "attacks" (attempts to break the cipher) it can withstand. The most difficult type of attack to withstand is called the "chosen plaintext attack." In this type of attack, an adversary is able to submit any amount of plaintext to the encryption algorithm and obtain the corresponding ciphertext. The (P,C) pairs can then be used to try to determine the secret key and break the cipher.

An encryption scheme that is used as a standard should be able to withstand chosen plaintext attacks, especially if the algorithms E and D are published as part of the standard. The strength of an encryption scheme is determined by the algorithm itself and by the complexity of the secret information (in the case of modern encryption schemes, by the length of the key). In general, longer keys (i.e., more digits or binary bits) correspond to a stronger cipher, but this is not necessarily the case: for a given algorithm, a shorter key weakens the cipher, but for different algorithms, one using a shorter key may be stronger overall than one using a longer key length.

The strength of any encryption scheme rests fundamentally on the integrity of the key(s) used. Therefore, proper key management is fundamental to the security provided by any encryption scheme or cipher.[4]

Evolution of the Data Encryption Standard

The Solicitation for a Standard

No single event or act of Congress led the Federal Government to adopt a published encryption standard for Federal agencies to protect their unclassified computer data and communications. Instead, a number of developments and concerns came together in the 1960s and 1970s that caused many people in and out of Government to conclude that a common means of protecting the Government's electronic information was needed.

One of these developments was the Brooks Act of 1965 (Public Law 89-306), which authorizes the National Bureau of Standards (NBS) to develop standards governing the purchase and use of computers by the Federal Government, to do research supporting the development of these standards, and to assist Federal agencies in implementing them. At the same time there was an increasing interest in ensuring the confidentiality and security of the Federal Government's computer files containing data on individual citizens.[5] Additionally, electronic transactions, such as fund transfers, were beginning to proliferate both within the Federal Government and in the private sector.

---

[1] See, for example, David Kahn: *The Codebreakers: The Story of Secret Writing* (New York, NY: The MacMillan Co., 1967).

[2] These are called symmetric encryption algorithms. Asymmetric ciphers also exist, such as the "public-key" algorithms. (See the discussions in ch. 4 and app. D.)

[3] See R.C. Summers, "An Overview of Computer Security," *IBM Systems Journal*, vol. 23, No. 4, 1984, pp. 309-325.

[4] See the discussion of key management in ch. 4.

[5] These concerns were addressed in the Privacy Act of 1974, for example. For more background on DES, see: U.S. Senate Select Committee on Intelligence. "Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard" (Staff Report), 98th Cong., 2d sess., April 1978.

These trends gave impetus to growing concerns for the security of Federal electronic information and transactions. A consensus developed among computer security researchers at NBS and the National Security Agency (NSA) that a technical means should be developed for safeguarding them against accidental error as well as from assaults by organized crime. At the time, they anticipated that the useful lifetime of this safeguard technology would be about 30 years—until the late 1990s.[6]

NBS initiated a study in 1968 to evaluate the Federal Government's computer security needs. As a result, NBS decided in 1972 to develop a governmentwide standard for encrypting unclassified Government data using an encryption algorithm to be published as a public standard. NBS initiated a computer security program within its Institute for Computer Sciences and Technology (ICST) in mid-1972. In early 1973, NBS and NSA staff met to discuss the encryption project. Throughout the development of the standard, NBS made use of NSA's recognized expertise, including the evaluation of algorithms proposed for the standard. Also, some technical personnel left NSA and joined NBS during the early 1970s to staff the latter's new computer security program. A chronology of DES development, provided by NBS, is shown in table 15.

On May 15, 1973, NBS issued a solicitation through the *Federal Register* for interested parties to submit algorithms for possible consideration as a data encryption standard. There were few responses; none were considered suitable. A second solicitation was issued on August 27, 1974. IBM responded to the second solicitation; its algorithm eventually became the Data Encryption Standard (DES).

IBM had already done considerable work developing encryption algorithms. Prior to the solicitation for DES, IBM had developed and patented a 64-bit Cash Issuing Algorithm for safeguarding financial transactions and a 128-bit encryption algorithm called Lucifer.[7] As part of the patenting process, IBM's algorithms were submitted to NSA for review to determine whether or not the algorithms should be classified. NSA chose not to classify the algorithms and suggested to IBM that one of them, with some modification, should be submitted to NBS.

This step in the process has given rise to a great deal of controversy over the years. Although the algorithm that IBM submitted to NBS was exactly that which was published later as the Data Encryption Standard, this algorithm differed from the original IBM algorithm in a couple of fundamental ways. These changes were made by IBM on the advice of NSA, which later led to questions as to whether NSA had "tampered" with the algorithm or weakened it in some way, perhaps creating a "trapdoor" that NSA could spring. First, the key length was shortened to 56 bits. Second, changes

---

[6] D. Branstad, NBS ICST. Private communication with OTA staff, Aug. 6, 1986.

[7] For a discussion of Lucifer and a description of the algorithm, see: Horst Feistel, "Cryptography and Computer Privacy," *Scientific American*, vol. 228, No. 5, May 1973, pp. 15-23.

Table 15.—Chronology of DES Development (major Federal agency events)

Event	Date
• NBS identifies need for computer security standards	August 1971
• NBS initiates program in computer security	July 1972
• NBS meets with NSA on encryption project	February 1973
• NBS publishes request for encryption algorithms	May 1973
• NSA reports no suitable algorithms were submitted	December 1973
• NBS publishes second request for algorithms	August 1974
• NSA reports one submitted algorithm is acceptable	October 1974
• NSA approves publication of proposed algorithm	January 1975
• DOJ approves publication of proposed algorithm	February 1975
• NBS publishes proposed algorithm for comment	March 1975
• NBS publishes proposed DES for comment	August 1975
• NBS briefs DOJ on competition issues	February 1976
• NBS holds workshop on technology concerning DES	August 1976
• NBS holds workshop on mathematical foundation of DES	September 1976
• DOC approves DES as a FIPS	November 1976
• NBS publishes DES as FIPS PUB 46	January 1977

SOURCE: National Bureau of Standards, circa 1978.

were made in the internal structure of the substitution functions—often referred to as the "S-boxes" —contained within the algorithm.[8]

In response to these concerns, NSA publicly stated that the reduced key size was sufficient for use in unclassified applications and, furthermore, that the IBM algorithm proposed for the data encryption standard was "to the best of their knowledge, free of any statistical or mathematical weakness."[9] However, it was difficult for individuals outside of NBS, NSA, or IBM to independently substantiate (or refute) these statements. At the request of NSA, IBM had not disclosed all of the design criteria used in the creation of the candidate algorithm—in particular, those resulting from NSA's testing and evaluation of the original algorithm and the criteria that had been used to select the modified S-boxes and shorter key length. Thus, although the proposed DES was published for comment, not all of the evaluative criteria that has been used in developing the algorithm were made public.

Comments on the Proposed Standard

Comments on the proposed standard were solicited in the *Federal Register* on March 17 and August 1, 1975, and in an August 1, 1975 letter sent to all Federal Information Processing Standards points of contact in Federal agencies.[10] NBS prepared an analysis of the comments from the three solicitations.[11] According to NBS, "all responses have been carefully considered and changes made to the standard where appropriate. However, no changes have been made to the algorithm itself and no substantive changes have been made to the standard which would warrant further solicitation for comments."[12] (See box F.)

One of the specific recommendations contained in the comments was that only hardware implementations should be considered. In response, NBS stated that "hardware is the only recommended implementation."[13] Nevertheless, several software implementations of DES have been developed by vendors for use by the private sector;

Box F.—Data Encryption Standard Summary of General Concerns

The following is a summary of the substantive general concerns about the proposed Data Encryption Standard stated in the comments received by NBS:

1. Computer equipment and related data processing equipment not based on a 64-bit architecture will be placed at a competitive disadvantage (A2, A3, A4, A5, A9, A10, B2, B5, B7, B10).
2. Certain types of communication systems may be degraded to a significant degree (A1, A2, A3, A4, A5, A10, A11, B2, B4, B5, B9).
3. The proposed algorithm is too complex, especially when implemented in software (A1, A3, A4, A8, A10, A11, B4, B9).
4. Applicability of the algorithm, including when and where to use it, is not specified (A11, B2, C2, C6).
5. The proposed standard does not contain information on electrical, mechanical and functional interfaces to devices implementing the standard (A2, A7, A9, B2, B5, B7, C2, C6).
6. Administrative procedures for validation, procurement and testing have not been described (A1, A4, A7, B2, C2, C6).
7. Policy for exporting devices implementing the proposed DES has not been made (B2).
8. The algorithm does not provide an adequate level of security (A2, A3, A4, A6, A8, B7, B9, B10).

SOURCE: "Analysis of Comments on the Data Encryption Standard," unpublished data available for public review at NBS.

---

[8] These were some of a set of allegations to the effect that NSA was improperly involved in the development of DES and was attempting to exert undue influence on university and private-sector cryptological research. The Senate Select Committee on Intelligence conducted a classified investigation of these allegations. Among its findings was that: "NSA did not tamper with the design of the algorithm in any way. IBM invented and designed the algorithm, made all pertinent decisions regarding it, and concurred that the agreed upon key size was more than adequate for all commercial applications for which the DES was intended." U.S. Senate, Select Committee on Intelligence, "Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard" (Staff Report), 95th Cong., 2d sess., April 1978, p. 4.

Others contend that the modifications that were made to the S-boxes improved them and also were, at least in part, intended to minimize their logic to permit a smaller chip size when DES was implemented in hardware.

[9] U.S. Senate Select Committee on Intelligence, April 1978, op. cit.

[10] The Department of Commerce/NBS published the proposed Data Encryption Algorithm in the *Federal Register* on Mar. 17, 1975 (vol. 40, No. 52, p. 12134 et. seq.) and solicited comments to be submitted to NBS by May 16, 1975.

[11] "Analysis of Comments on the Data Encryption Standard," NBS/ICST (n.d., circa 1978). In total, 18 industry, 10 Federal, and 1 congressional source responded. Copies of all comments received by NBS and NBS' responses are available for public review at NBS.

[12] Ibid.

[13] Ibid.

the first software simulation of DES (by Computation Planning, Inc.) was announced in November 1975.

The previously mentioned controversy and debate concerning the strength of the proposed standard and NSA's role in its development continued through the 1970s. To address some of these concerns, NBS sponsored two workshops on DES and also briefed the Department of Justice concerning possible competition issues involving the proposed standard. The first workshop, held in August 1976, addressed the technical and economic feasibility of constructing a special-purpose computer to attack DES through computational brute force. The second workshop, held in September 1977, addressed the mathematical foundations of the DES algorithm. Although the outcome of these workshops was to allay most fears that DES was not sound or could be inexpensively broken by brute force before the 1990s, participants expressed concerns that it had not been possible to assess all of the design characteristics of DES because some had not been made public.[14]

Also, in late 1975, Congressman Jack Brooks (D-Tex.), writing in response to the solicitation for comments, asked whether NSA had put undue influence on NBS in setting the security level of DES and what the NBS role had been in DES development and key generation. Prompted by Brooks' inquiry, the Senate Select Committee on Intelligence staff ultimately responded, after a classified inquiry, that there had been no undue NSA influence.[15] At the time, NBS stated that, although it would provide guidance and good techniques for individual Federal agencies to generate their own DES keys in accordance with Federal Information Processing Standards (FIPS), no Government agency should generate keys for other agencies or for the private sector.

Promulgation of the Standard

The Department of Commerce approved DES as a standard in November 1976. NBS published it as FIPS PUB 46 in January 1977, with the provision that DES would be reviewed for continued suitability at 5-year intervals and would be recertified (or not) every 5 years by NSA. DES was last recertified in 1982.

The administrative and technical workloads associated with the development and promulgation of DES were substantial—for NBS; other Federal agencies; the private sector (including vendors, the banking community, university researchers, and others); and for Congress, its staff, and support agencies. According to NBS, DES consumed some 3 man-years of effort for DES-related interactions alone by 1978, exclusive of IBM's technical development of the algorithm. Although exact statistics were not compiled, these interactions included a conference at NBS and some 2,000 technical and policy meetings, telephone discussions, and mail contacts. A 3-year projection of continued interactions more than tripled the man-year estimates.

Developing the standards to support DES—for use in communications, data storage, message authentication, user/terminal authentication, physical security, magnetic stripe encryption, and key management—consumed an estimated 6½ man-years at NBS and another 34 man-years elsewhere between 1977 and 1980.[16]

One estimate of the total (administrative, technical, test, and validation) DES-related costs through 1977 amounted to about $515,000 for NBS, some $6 to $10 million for IBM, about $460,000 for NSA, and around $1.5 million for other users and vendors. The estimated NBS support cost for DES during the period 1978-80 was more than $800,000.

As of January 1987, about 20 industry vendors had produced one or more versions of hardware or firmware devices (chips) implementing the DES algorithm, for use in their own products or for sale to other manufacturers. And, as of that date, NBS had validated 28 implementations of the DES algorithm in hardware or firmware, produced by 11 vendors.

NBS, which takes the position that software implementations of DES would not comply with the Federal standard, only validates electronic devices (hardware or firmware) implementing the DES algorithm. The rationale is that hardware implementations are faster than software and that they are thought to be more reliable and harder for an adversary to modify "behind the user's back."[17] Software implementations of DES are being marketed, but are not validated or certified for Government use. Also, some vendors choose not to submit their hardware or firmware DES products for validation or certification for Government use. According to NBS staff, the Department of Defense is one of the largest single Federal customers for DES-based devices.

---

[14] "Computer Encryption and the National Security Agency Connection," Science, vol. 197, July 29, 1977, pp. 438-440.

[15] U.S. Senate Select Committee on Intelligence, April 1978, op. cit.

[16] Source: Unpublished estimates developed at NBS in the late 1970s.

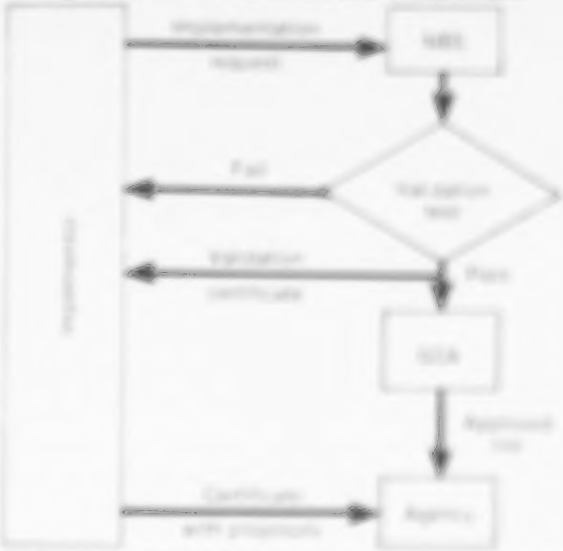
[17] At the same time, it is worth noting that software implementations of high-quality encryption are much more difficult to control in terms of their dissemination and exportability. Because the DES algorithm is published, almost anyone with the requisite technical skills can produce software versions of it; producing microprocessor-based implementations is more difficult. The new NSA secret algorithms are easier to control because they are not published.

Figure 22 shows the roles of NBS and GSA in DES-based product validation and procurement.

Description of DES

A short technical summary of the encryption algorithm used in DES is given in figure 13 and box B of chapter 4. Complete technical descriptions of the four DES modes of operation, including initialization and error propagation properties and use for message authentication, may be found in FIPS Publications 74, 81, and 113, issued by NBS.[14] Diagrams of DES modes of operation, taken from NBS publications, are given in figure 23.

Figure 22.—DES Validation and Procurement

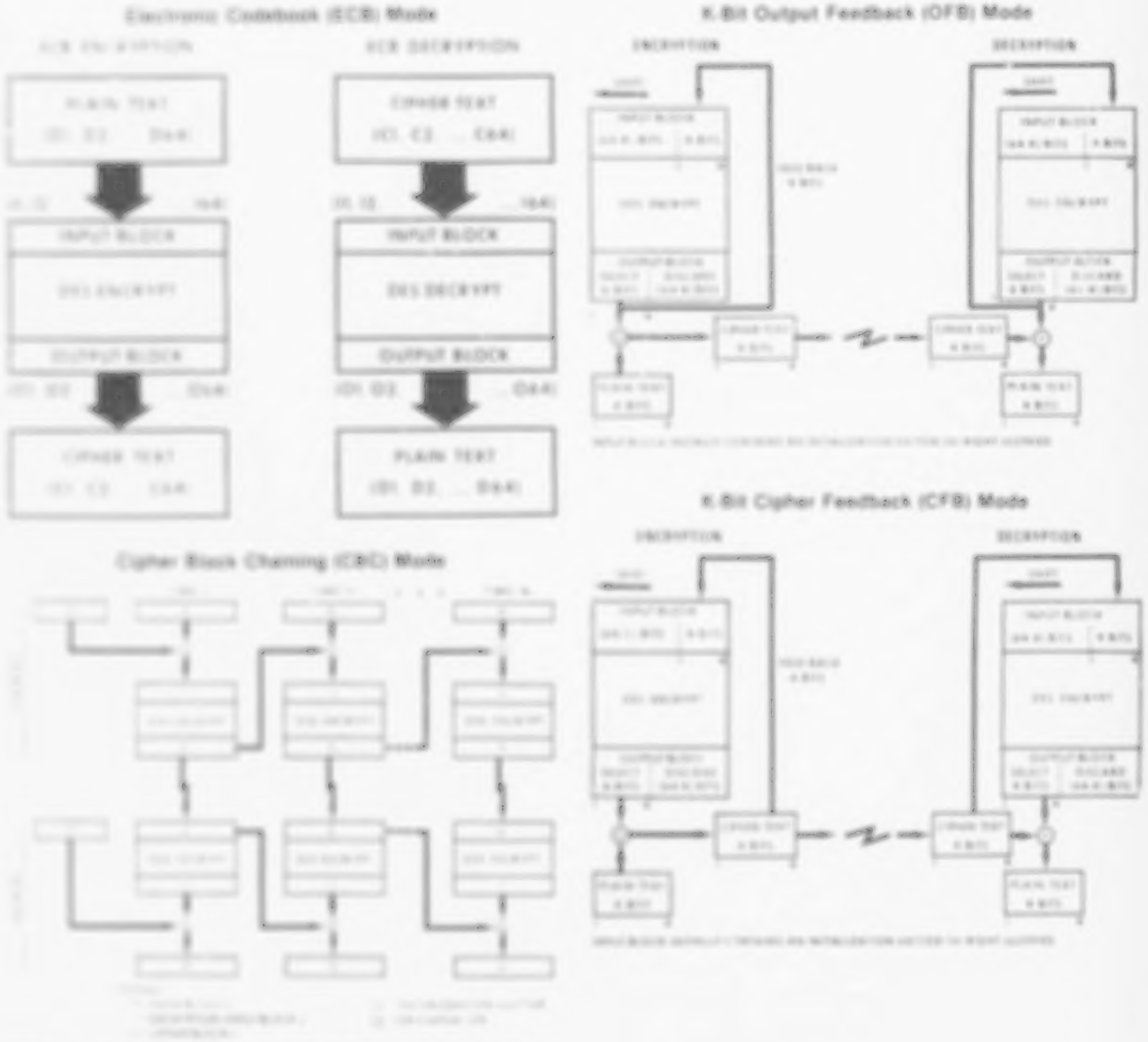


SOURCE: National Bureau of Standards/Institute for Computer Sciences and Technology.

---

[14] U.S. Department of Commerce, National Bureau of Standards, "Guidelines for Implementing and using the NBS Data Encryption Standard," FIPS PUB 74, Apr. 1, 1981; "DES Modes of Operation," FIPS PUB 81, Dec. 2, 1980; and "Computer Data Authentication," FIPS PUB 113, May 30, 1985.

Figure 23.—DES Modes of Operation



SOURCE: National Bureau of Standards, FIPS PUBS 81 and 74, Apr. 1, 1981.

Appendix D

Message Authentication, Public-Key Ciphers, and Digital Signatures

Message Authentication

An "authentic" message is one that has arrived exactly as it was sent (without errors or alterations), is not a replay of a previous message, and comes from the stated source (not forged or falsified by an imposter or fraudulently altered by the recipient).[1] Encipherment in itself does not automatically authenticate a message: it protects against passive eavesdropping automatically, but does not protect against some forms of active attack.[2]

Encipherment algorithms can be used to authenticate messages, however, and the algorithm used in the Data Encryption Standard (DES) is the most widely used cryptographic basis for message authentication. As discussed in more detail later, there are profound differences in using a symmetric cipher, such as the current DES algorithm, rather than an asymmetric one like the RSA algorithm named after its inventors: Ronald Rivest, Adi Shamir, and Leonard Adelman. Use of a symmetric cipher for message authentication can only protect against third parties and not against fraud by either the sender or receiver (both of whom know the secret key), while an asymmetric algorithm can be used to resolve disputes between the sender-receiver pair.

As the uses of electronic media for financial and business transactions have proliferated, message authentication techniques have become increasingly important and have evolved from simple pencil-and-paper calculations to sophisticated, high-speed hardware processors.

In general, the various message authentication schemes that are used can be grouped together according to whether they are based on public knowledge or, at least in part, on secret knowledge. Among the former are message authentication using check fields,[3] parity checks,[4] and cyclic redundancy checks.[5] These share a common weakness: unauthorized or fraudulent modifications may go undetected because they are accompanied by matching, yet fraudulent, authentication parameters that can be calculated by unauthorized parties because the authentication parameters are not secret.

Using secret authentication parameters known only to the sender and receiver permits a stronger form of message authentication because the check field data cannot be forged by a third party unless the secret parameters are compromised. A different secret parameter is usually required for each sender-receiver pair. The logistics for distributing this secret information to the correct parties is analogous to key distribution for encryption. Compromise of the secret parameters invalidates the integrity of the safeguarding function because it could then be forged. (See ch. 4.)

---

[1] For a thorough discussion of message authentication and the various techniques used to authenticate messages, see Davies & Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Fund Transfers* (New York, NY: J. Wiley & Sons, 1984) ch. 5. The descriptions of authentication techniques in this section follow Davies & Price closely.

[2] Davies & Price describe passive attack as eavesdropping and active attack as the falsification of data and transactions through such means as: 1) alteration, deletion, or addition; 2) changing the apparent origin of the message; 3) changing the actual destination of the message; 4) altering the sequence of blocks of data or items in the message; 5) replaying previously transmitted or stored data to create a new false message; or 6) falsifying an acknowledgment for a genuine message. (See Davies & Price, op. cit., pp. 119-120.)

[3] Check field techniques are designed to ensure that stored or transmitted information has been prepared correctly. A check field is a simple function of the numerical characters in the important fields of the message that makes it highly likely that the most common types of mistakes and errors will be detected. The use of check fields does not safeguard against deliberate fraud by data-entry operators or others: because the check sum function and the data used to create it are not secret, a data-entry operator could calculate the "correct" check sum and transmit it along with a fraudulently altered message. Also, it is possible to generate false messages that have the same calculated check sum value as the original message. (See Davies & Price, op. cit., pp. 121-122.)

[4] Parity checks can be used to detect accidental errors during transmission, usually either by using an eighth "parity" bit with each seven-bit message word or by providing longitudinal parity checks using modulo-2 addition on successive words. Parity checks are weak in that multiple errors and/or missing blocks can sometimes go undetected. (See Davies & Price, op. cit., p. 122.)

[5] According to Davies & Price, cyclic redundancy checks are the best known error detection method and offer strong protection against accidental error. However, the procedure for creating the check data via a predetermined polynomial is public knowledge. Therefore, the checks do not provide strong protection against an active attack. In this form of message authentication, the cyclic check operation calculates the check data by dividing the polynomial formed by a block of message bits by the predetermined check polynomial and using the "remainder" from the polynomial division as a check field. The check field is appended to the message block and transmitted with the message. Upon its receipt, the recipient performs the same polynomial division operation on the message and compares the remainder with the transmitted check field to authenticate the message. The cyclic check does not protect against active attack because the means of creating the check data—the polynomial division operation—is not secret. An active wiretapper can divert the message, alter it, calculate a new check field using the correct predetermined polynomial, and retransmit the altered message with the new check field appended. The message will appear to be authentic when the recipient compares the check fields. (See Davies & Price, op. cit., pp. 122-123.)

In the most general sense, an authentication function based on secret knowledge can be constructed from a public authenticator algorithm and a secret authentication key.[6] Examples of authenticators based on secret keys include the Decimal Shift and Add (DSA) algorithm,[7] and the proprietary S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunications) and Data Seal algorithms, which use binary arithmetic.[8] Although authentication can be based on encryption (the DES algorithm, for example, is widely used for message authentication), the strict requirements for an authenticator algorithm differ from those for an encryption algorithm because authentication does not require the existence of an inverse function (i.e., decryption). It is also possible to base message authentication on secret numbers used in conjunction with special one-way functions.[9]

Encryption alone is not always sufficient to completely authenticate a message. If decryption of an encrypted message yields "sensible" plaintext, without garbled portions, then there is reasonable certainty that the message was originated by the other "authorized" holder of the secret key. However, some types of message alterations can go undetected.[10] A more robust authentication method (than DES encryption alone, for example) is to use DES hardware in an appropriate mode of operation in order to create a message authentication code.[11]

When DES hardware is used for authentication, it is operated in either the cipher block chaining (CBC) or cipher feedback (CFB) mode; the chaining or feedback operation ensures that the authenticator, selected from the last state of the DES hardware output register, is a function of the entire message stream input to the DES device.[12] The authenticator is appended to the message and transmitted along with it. The recipient removes the authenticator from the received message and calculates his or her own value of the authenticator using the secret key and initialization vector shared with the sender. If the two authenticator values are the same, then there is increased assurance that the message is authentic.

The message can be transmitted in plaintext without compromising its authenticity. If the message is altered by a third party who does not use the secret DES key to calculate a forged authenticator to append to the altered message, then the authenticator calculated by the receiver will not have the same value as the one transmitted with the message. However, because both sender and receiver know the secret parameters, either could fraudulently alter the message and deny having done so. This type of dispute can be resolved through use of an asymmetric cipher, as will be discussed below in the sections on public-key ciphers and digital signatures.

If privacy as well as authentication is required, then one scheme for encrypting and authenticating a message involves sequential use of DES using two different secret keys: one to calculate the authenticator (called the message authentication code or MAC), and one to encrypt the message. These operations can be performed in either order; the ANSI X9.23 standard requires that the MAC be calculated before encryption.[13] Even the MAC and encryption do not safeguard against replay of messages (e.g., electronic fund transfers). Therefore, various message sequence numbers or date and time stamps are usually incorporated into the text of the message. The ANSI X9.9 standard requires a message identifier field to prevent replay.

---

[6] For mathematical and functional descriptions of authenticator functions, see Davies & Price, op. cit., pp. 123-135; and R.R. Jueneman, S.M. Matyas, and C.H. Meyer, "Message Authentication," *IEEE Communications Magazine*, vol. 23, No. 9, September 1985.

[7] DSA is based on parallel computations performed by the sender and receiver; the starting point for the computations are two secret 10-digit decimal numbers. The message to be authenticated is treated as a string of decimal digits, thus DSA requires that alphabetic characters be encoded into numeric form, although the numeric content of a message (e.g., the value of a financial transaction) does not require any conversion. According to Davies & Price (see pp. 127-130 for an example of DSA), the algorithm can be implemented using a programmable decimal calculator.

[8] Because these are proprietary, they are not available for use as a published standard.

[9] A one-way function has the special property that, although the function itself is relatively easy to compute, its inverse is quite difficult to compute—i.e., even if the values of authenticators for many messages are known, it is almost impossible to recover the text of a message given only the value of its authenticator. Some, but not all, "hash functions"—functions that appear to generate random outputs from nonrandom inputs—are suitable for message authentication.

[10] See Davies & Price, op. cit., pp. 134-135 for examples. Jueneman, et al., also discuss strengths and weaknesses of various authentication and manipulation detection techniques.

[11] Strictly speaking, any block encryption algorithm could be used. However, in practice, the cipher used is DES because the algorithm is readily available in hardware form. The DES algorithm is relatively slow in software form, which makes the hardware form much more convenient for data transmission.

[12] In the CBC mode, the authenticator is the most significant *n* bits from the last block output by the device. In the CFB mode, the DES device is operated one additional time after the last message block is input, and the authenticator is selected as the most significant *n* bits of the final output block. The length of the authenticator (usually 32 bits for EFT authentication, according to the standard) is determined jointly by the sender and receiver.

[13] If the MAC checks the ciphertext, then an adversary is able to mount a known plaintext attack on the key used for authentication. If, however, the MAC checks the plaintext, then an adversary must break both the MAC key and the encryption key in order to send fraudulent messages.

Public-Key Ciphers

A symmetric cypher is an encryption method using one key, known to both the sender and receiver of a message, that is used both to encrypt and to decrypt a message. Obviously, the strength of a symmetric cipher depends on both parties keeping the key secret from others. With DES cipher, for example, for which the algorithm is known, revealing the encryption key permits the message to be read by any third party.

An asymmetric cypher is an encryption scheme using a pair of keys, one to encrypt and a second to decrypt a message.[14] A special class of asymmetric ciphers are public-key ciphers, for which the encrypting key need not be kept secret to ensure private communication.[15] Rather, Party A can publicly announce his encrypting key, PK_A, allowing anyone who wishes to communicate privately with him to use it to encrypt a message. Party A's decrypting-key, SK_A, is kept secret, so that only A (or someone else who has obtained the secret decrypting key) can easily convert messages encrypted with PK_A back into plaintext.[16]

Knowing the public encryption key—even when the encrypted message is also available—does not make computing the secret decrypting key easy, so that in practice only the authorized holder of the secret key can read the encrypted message.[17] However, with the encrypting key being publicly known, a properly encrypted message can come from any source, so there is no guarantee of its authenticity.

It is also crucial that the public encrypting key be authentic. An imposter could publish his own key, PK_I, and for example, pretend it came from A in order to read messages to A, which he could intercept and then read using his own SK_I. Therefore, the strength of the public-key cipher rests on the authenticity of the public-key and the secrecy of the private key. A variant of a public-key system allows a sender to authenticate messages by "signing" them using an encrypting key, which (supposedly) is known only to him. This is a very strong means of authentication and is discussed further in the following section on digital signatures.

Davies and Price[18] review and illustrate the functional requirements for a general public-key cryptosystem. A brief overview follows here, but a detailed description of the underlying mathematics is beyond the scope of this appendix.

If encipherment is performed by some function $E(K_e)$ and decipherment by another $D(K_d)$, then in order to make the decipherment function the inverse of encipherment, the encrypting key, K_e, and the decrypting key, K_d, must be related somehow. Suppose both keys are derived from a randomly selected starting key, or seed key, K, such that $K_e = F(K_S)$ and $K_d = G(K_S)$, where the functions F, G, D, and E defined above are published. Party A would then select a K_S (which would be kept secret), use it to calculate K_e and K_d, and publish K_e as his public key, PK_A, while keeping K_d secret as the secret key, SK_A.

If P is the plaintext message and C is the encrypted message, then $C = E(P)$ and $P = D(E(P))$; that is, $D(E(P))$ must be the inverse of E. However, because E is really the function $E(K_e)$ and is public, the function E must not be readily invertible or else an opponent can readily calculate P given C and E. This property is described as making E

---

[14] See Davies & Price, op. cit., ch. 8, for a more complete discussion of asymmetric and public-key ciphers.

A discussion of the underlying principles of public-key ciphers, including examples of the RSA and knapsack algorithms, is given in: Martin E. Hellman, "The Mathematics of Public-Key Cryptography," *Scientific American*, vol. 241, No. 2, August 1979, pp. 146-157.

A pictorial example of the RSA public-key method can be found in *Computer Security* (one of the *Understanding Computers* series) (Alexandria VA: Time-Life Books, 1986), pp. 112-117.

[15] The public-key concept was first proposed by Whitfield Diffie and Martin Hellman in "New Directions in Cryptography," *IEEE Trans. Information Theory*, IT-22, 6, November 1976, pp. 644-654. Diffie and Hellman also described how such a public-key cryptosystem could be used to "sign" individual messages and to simplify the distribution of secret keys. Their work was the basis for Rivest, Shamir, and Adelman's practical implementation of such a system in 1978, called the RSA cipher. Some ciphers proposed for public-key systems have subsequently been broken. For example, the Diffie-Hellman "discrete exponential" cipher was broken several years later by Donald Coppersmith of IBM [G. Kolata: "Another Promising Code Falls," *Science*, vol. 226, Dec. 16, 1983, p. 1224]. The "trap-door knapsack" cipher, another public-key cipher proposed in 1976 by Hellman and Ralph Merkle, was broken by Shamir and Adelman in 1982. (See *Computer Security*, op. cit., pp. 100-101; and Hellman's 1979 article in *Scientific American*.)

[16] This section uses the notation PK for "public key" (usually, the encrypting key) and SK for "secret key" (usually, the decrypting key). For A and B to have two-way communication, two pairs of keys are required: the "public" encryption keys PK_A and PK_B, and the secret decryption keys SK_A and SK_B.

[17] Use of the two keys might also be used to separate access to "read" and "write" data functions. For example, by controlling dissemination of the encryption key, one might control write access; by controlling dissemination of the decryption key, read access.

[18] Davies & Price, op. cit., ch. 8.

(and also the function F, which generates K_e from K_S) one-way functions that cannot readily be inverted.

The requirements that E be a noninvertible, one-way function and that D(E(P)) be its inverse are reconciliable when E is not invertible without knowledge of K_e, but the inverse of E is readily obtained using the secret key K_d. Thus, knowledge of the secret key is a "trapdoor," which makes the inverse of E simple to implement. E(P), where $E = E(K_e)$, is a one-way function with a trapdoor D(E(P)), which allows it to be inverted. Knowledge of K_d springs the trapdoor.[19]

A public-key cryptosystem consists of encryption and decryption functions, together with methods for generating pairs of keys from the random seed values. The one-way property of a "one-way function," such as E, is really only a matter of computational complexity. The encryption function should be relatively easy to carry out, given K_e and E, but given the ciphertext $C = E(P)$, the plaintext $P = D(E(P))$ should be very hard to calculate and should require a very large number of steps, unless K_d is known.

In principle, it should be possible to calculate values of C for many values of P and then to sort and tabulate the pairs of (P_i, C_i) to obtain an explicit inversion of E. Because this type of exhaustive search process requires a large number of computational steps and large computer memory size, both of which grow exponentially with the key size, E is effectively a one-way function if the explicit inversion requires a very large number of (P,C) pairs.

Like all of modern cryptography, public-key cryptosystems rely heavily on mathematics and, in particular, on number theory. The RSA cipher is based on modular arithmetic[20] and the trapdoor knapsack cipher is based on combinatorial mathematics as well. The mathematical problems underlying the RSA cipher and the knapsack public-key cipher belong to a class of problems called "nondeterministic, polynomial-time problems," or NP problems. The computational burden of finding a solution to the hardest NP problems, using published methods, grows very rapidly as the size of the problem increases. It is strongly believed (but not proved) that the burden must grow very rapidly, no matter what method of solution is used. However, once the solution is found, it can be checked very easily.[21] Even so, it is possible that advances in mathematics and computer science may undermine public-key cryptosystems based on "one-way" functions. One instance of this was the "breaking" of the trapdoor knapsack cipher. Box G describes this cipher.

The knapsack cipher system was thought to be effectively unbreakable (computationally but not unconditionally secure) and Merkle issued an open challenge to cryptologists in 1976 to break it. In 1982, Adi Shamir at the Massachusetts Institute of Technology (MIT) broke the cipher analytically. Soon afterward, Leonard Adelman, a former colleague of Shamir, used Shamir's method and an Apple II computer to break an example of the knapsack cipher.

Another public-key system, called the RSA system, was announced in 1978. The RSA system is computationally more complex to implement than the trapdoor knapsack cipher and it has not yet been broken. Also, the RSA system does not expand the plaintext message the way the knapsack cipher does. Message expansion occurs with the knapsack cipher because the sum of the "hard" knapsack vector used in the knapsack public key is larger than the sum of the "easy" vector used in the secret key. Therefore, more binary bits are required to represent the ciphertext than to represent the plaintext.

The RSA Public-Key System

The RSA public-key system is thought to be the most computationally secure, commercially available public-key system. It also enables the prob-

---

[19] See Davies & Price, op. cit., ch. 8 for a more thorough explanation. Diffie and Hellman introduced the concept of trapdoor one-way functions in their 1976 paper (op. cit.), but did not present any examples. In their 1978 paper, Rivest, Shamir, and Adelman presented their implementation of a public-key system using a one-way trapdoor function. See also R.L. Rivest, A. Shamir, and L. Adelman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, No. 2, February 1978; and Hellman's article in the August 1979 issue of *Scientific American* op. cit.

[20] Finite arithmetic with modulus *m* (modular arithmetic) has the operations of addition, multiplication, subtraction, and division defined. A *prime number*—e.g., 3, 5, or 7 in modulo 10 arithmetic—has no factors other than 1 and itself. Finite arithmetic with a *prime modulus p* has the additional property that multiplication always has an inverse. This property is crucial for cryptography.

In modulus 10 arithmetic, for example, the number 57 would be represented by its remainder, 7: 57/10 = 5, with a remainder of 7. More generally, the remainder always has a value between 0 and (m − 1), where *m* is the modulus. Thus, in modulus 3 arithmetic, 57 would be represented by the remainder of 0; in modulus 11 arithmetic by the remainder of 2, etc.

The exponential function a^x in modulus *p* arithmetic is valuable as a one-way function: calculating the exponential $y = a^x$ is easy, but calculating its inverse, $x = \log_a y$ is difficult for large *p*.

[21] See Hellman's article in the August 1979 *Scientific American*, op. cit.

Box G.—The Trapdoor Knapsack Cipher

The trapdoor knapsack system was proposed by Ralph Merkle and Martin Hellman in 1976.[1] The "knapsack puzzle" or "knapsack problem" is well-known in mathematics and can be summarized briefly as the following problem:

> Suppose you are given a set of N weights of assorted (and known) integer sizes. You want to use them to balance a knapsack that holds an unknown combination of the same weights. You are given the values of the set of integer weights (called the knapsack vector) and the weight to be matched (called the knapsack total). Find the subset of the N weights that will exactly balance the knapsack!
>
> Although it is possible to find examples of this problem that are fairly easy to solve by exhaustive search—when N is a small number or when each weight is heavier than the sum of the proceeding weights, for example—all of the known methods of solving the general knapsack problem have a computational requirement that grows exponentially in the key size and, therefore, are impossible to implement for reasonably large key sizes. An exhaustive search is quite lengthy for large N. Suppose that N is 5. Then, the knapsack vector has five components (one corresponding to each weight), each of which could be equal to 1 (the weight is used to try to balance the knapsack) or 0 (the weight is not used in this try). There are 2^5 or 32 possible vectors to be tried in an exhaustive search. If N were 10, up to 1,024 tries would be covered in an exhaustive search. If N were 1,000, an exhaustive search would clearly be infeasible.
>
> Sometimes the problem is posed differently, as a cylindrical knapsack of fixed length and a set of rods of different lengths, with the problem being to find the subset of rods that will completely fill the knapsack. In either case, the problem is an example of the general class of NP problems. The "trapdoor" knapsack problem is a special case, which is not computationally difficult to solve provided that one has special information that enables the problem to be solved more easily than for the general case. In this case, the "trapdoor" enables the intended recipient who knows the secret key (the trapdoor information) to solve the knapsack problem and reveal the plaintext message without having to do an exhaustive search.

The intended receiver and originator of the public and secret keys builds a secret structure into the knapsack problem. The receiver generates the keys by first generating an "easy" knapsack vector, called a super-increasing vector, in which each weight is larger than the sum of the preceding weights. The sum of the super-increasing knapsack vector is the heaviest possible knapsack. The receiver then chooses a modulus *m* larger than this maximum weight and a multiplier *a* such that *m* and *a* are relatively prime. The "hard" knapsack vector is constructed by multiplying the "easy" vector by *a*, using modulus *m* arithmetic. The "hard" knapsack vector, arranged in order of increasing weight, forms the public (encryption) key. The "easy" vector, along with the values used for *m* and *a*, are kept as the secret key.

Merkle and Hellman's public-key system was based on special key pairs that were used to encrypt and decrypt plaintext. Briefly (see *Computer Security*, pp. 100-101), each character in the plaintext was assigned a numerical value and all the numbers were then summed together. The secret key enabled the individual numbers to be recovered and, from them, the plaintext.

---

[1] For the history of the trapdoor knapsack system, see *Computer Security*, one of the *Understanding Computers* series (Alexandria, VA: Time-Life Books, 1986), pp. 100-101; Davies & Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*, (New York, NY: J. Wiley & Sons, 1984), p. 251; and Martin E. Hellman, "The Mathematics of Public-Key Cryptography," *Scientific American*, vol. 241, No. 2, August 1979, p. 148.

lem of disputes between sender and receiver to be resolved through the method of digital signatures.[22]

The RSA system is based on a problem that is even older than the knapsack problem: that of "factoring" a large number (finding all the prime numbers that divide it evenly).[23] This is another computationally "one-way" problem in that factoring a large number takes much longer (by hand or by computer) than does verifying that two or more numbers are prime factors of the same large number.

The proprietary RSA system is thought to be based on the relative difficulty of finding two large prime numbers, given their product. The recipient (and originator of the key pair) randomly selects two large prime numbers, called p and q. These prime numbers are kept secret. Another (odd) integer e is chosen, which must pass a special mathematical test based on values of p and q. The product, n, of p times q and the value of e are announced as the public encryption key. Even though their product is announced publicly, the prime factors p and q are not readily obtained from n. Therefore, revealing the product of p and q does not compromise the secret key, which is computed from the individual values of p and q.[24]

The RSA public (encrypting) key consists of two integers, n and e, where n is the product $n = (p)(q)$. If each block of the plaintext message is represented as an integer between 0 and $(n-1)$, then encryption is accomplished by raising the plaintext to the eth power, modulus n.

The secret (signing and/or decrypting) key, d, is computed from p, q, and e as the "multiplicative inverse" of e, modulus $(p-1)(q-1)$; that is, the product of d and e is 1, modulus $(p-1)(q-1)$. Thus, individual knowledge of p and q are thought to be necessary to create the secret key. Decryption is accomplished by raising the ciphertext to the dth power, modulus n.

It is possible to break the RSA cipher if the prime factors p and q can be determined by factoring the value of n that was given in the public key. Many factoring algorithms exist, some based on the work of Fermat, Legendre, and Gauss. Others have been developed more recently to take advantage of computers and special processors to do fast factorization.

Depending on the factorization method used, it is possible to estimate the number of computational steps required to factor a number, n. The number of steps and the speed with which they can be performed determine the time required to factor n. The number of steps required to factor n—thus, the work and time required to "break" the RSA cipher by the factorization approach (finding p and q)—increases rapidly as the number of digits in n increases.[25] Thus, an important feature of the

---

[22] Other public-key systems have been developed, some earlier than RSA, but have not gained as wide an acceptance in commercial markets. There continue to be new developments in public-key cryptography (see, e.g., S. Goldwasser, S. Micali, and R. Rivest, MIT Laboratory for Computer Science, "A Digital Signature Scheme Secure Against Adaptive Chosen Message Attack, Rev. Apr. 23, 1986), but some of these are of more academic interest than immediate practicability for safeguarding communications.

[23] For discussions of the underlying mathematics, see Davies & Price, op. cit., ch. 8; Rivest Shamir, and Adelman in the February 1978 *Communications of the ACM*, and Hellman in the August 1979 *Scientific American* op. cit.; *Computer Security*, op. cit., pp. 112-115, has an illustrated example.

The relationship between the RSA exponential functions used to encipher and decipher follows from an identity due to Euler and Fermat which demonstrates the properties that e and d must have, given p and q.

[24] Certain special values of $(p)(q)$ can be factored easily—when p and q are nearly equal, for instance. These special cases need to be avoided in selecting suitable keys.

[25] According to Davies & Price, op. cit., pp. 242-244, theory shows that, for the better-known factorization algorithms, the relationship between the number of steps and n is exponential. In the early 1980s, experimental work doing fast factorization using a number of techniques, including special processors, pointed to a "limit" of 70 to 80 decimal digits for factoring in one day.

Advances in theory and in microprocessor and computer technologies can serve to make estimates of this type obsolete. For example, Rivest, Shamir, and Adelman's 1978 article in the *Communications of the ACM* (February 1978, p. 125) provided a table estimating the number of operations required to factor n using the fastest-known method then. Assuming that a computer was used and that each operation took one microsecond, the authors estimated that a 50-decimal-digit value of n could be factored in under 4 hours, a 75-digit value in 104 days, a 100-digit value in 74 years, and that a 200-decimal digit n would require almost 4 billion years to factor.

RSA cipher is that the desired level of security (measured by the work required to break the cipher, or its "work factor") can be tailored from a wide range of levels simply by varying the number of digits in the key.

Davies and Price report on a new factorization method using parallel computation by special, large-scale integration (LSI) devices. Assuming that the parallel LSI devices use 128-bit arithmetic and run off a 10-MHz clock, a 100-decimal-digit value of *n* would take a little over 2 years to factor, a 150-digit *n* would take 6,300 years to factor, and a 200-digit *n* would take 860,000 years to factor.[26] Current implementations of the cipher use keys of 200 digits or longer; that is, the number *n* has 200 or more decimal digits.

Rivest, Shamir, and Adelman formed RSA Data Security, Inc., in 1982 and obtained an exclusive license for their invention from MIT, which owned the patent.[27] RSA Data Security has developed proprietary software packages implementing the RSA cipher on personal computer networks. These packages, being marketed commercially, provide software-based communication safeguards, including message authentication, digital signatures, key management, and encryption. Another offering is designed to safeguard data files and spreadsheets being transmitted between intelligent workstations, electronic mail networks, and files being stored locally. The RSA Data Security package that safeguards electronic mail and spreadsheets sells for about $250, including one copy of the program, a key generating program, and a registered and authenticated user identification number.

Digital Signatures

Encryption or message authentication alone can only safeguard a communication or transaction against the actions of third parties. They cannot fully protect one of the communicating parties from fraudulent actions by the other (forgery or repudiation of a message or transaction, for example) and cannot in themselves resolve contractual disputes between the two parties. Paper-based systems have long been based on mechanisms like letters of introduction for identification of the parties, signatures for authenticating a letter or contract, and sealing a (physical) envelope for privacy. The contractual value of paper documents hinges on the recognized legal validity of the signature and on the laws against forgery.

It is possible to provide equivalent functions for electronic documents by using a digital signature to authenticate the contents and also prove who originated the document (because only one party knows the secret information used to create the signature). A digital signature can be created using a symmetric cipher (such as DES), but in general asymmetric ciphers provide for more efficient operations. The digital signature method in most common use commercially is based on the RSA cipher.[28] The digital signature can be used with encipherment if privacy is required.

The equivalent of a "letter of introduction" is still necessary to verify that the correct public key is used to check the digital signature since an adversary might try to spoof the signature system by substituting his or her own public key and signature for the real author's. This letter of introduction could be accomplished by several means. The RSA Data Security system provides "signed key server certificates" by attaching the corporation's own digital signature to the users' public keys so that users can attach their certified public signature keys to their signed messages. Note that although a public-key cipher system is used to set up the digital signature system, the actual text of the message can be sent in plaintext, if desired, or it can be encrypted using DES or the public-key cipher.[29]

The RSA Data Security digital signature system works as follows:

First, a cryptographic "hashing" algorithm creates a shorter, 128-bit "digest" of the message. The message digest, similar to a checksum, is virtually unique[30] to each text. If a single bit of the plaintext message is altered, the message digest will change substantially. A one-way hashing function is used to prevent the document from being reconstructed from the digest.

---

[26] See Davies & Price, op. cit., pp. 243-244.

[27] Other university research in cryptography has also been patented and licensed. For instance, Stanford University has four cryptography patents available for licensing on a non-exclusive basis, for a wide range of potential applications (including protection of tape and disk drives; time-shared computers; satellite, microwave, and mobile radio communications equipment, computer terminals; and electronic banking). Stanford University considers that one of these patents (Public Key Cryptographic Apparatus and Method, U.S. Patent #4,218,582, Aug. 19, 1980, Martin E. Hellman and Ralph C. Merkle), covers any public-key system in any implementation.

Source: Letter dated 9/29/86 to OTA from Lisa Kuuttila, Stanford Office of Technology Licensing, Re: Stanford Dockets S77-012,-015, -048; S78-080, "Encryption Technology."

[28] See Davies & Price, op. cit., ch. 9, for a general treatment of digital signatures and alternative methods.

[29] For example, if the RSA digital signature is used to sign and encrypt, the sender's secret key is used to sign the message and the intended recipient's public key is used to encrypt the message. The recipient uses his secret key to decrypt the message and the sender's public key to check the signature. In practice, the RSA digital signature system is used to transmit a DES key for use in encrypting the text of a message because DES can be implemented in hardware and is much faster than using the RSA algorithm to encrypt text in software.

Next, the message digest is encrypted with the author's secret key.[31] In the RSA system, each key is the inverse of the other; that is, each key can decipher text enciphered with the other key. Therefore, using Party A's public key to decipher a message into sensible plaintext proves that Party A's secret key was used to encipher the message. The integrity of this system hinges on preventing the secret key from being compromised and ensuring that an imposter does not post his own public key and pretend that it is the real Party A's.

The enciphered message digest is attached to the text and both are sent to the intended recipient. The recipient removes the appended message digest and runs the text of the message through the same hashing function to produce his own copy of the message digest. Then, the recipient deciphers the message digest that was sent along with the message, using the supposed author's public key.

If the two message digests are identical, then the message did indeed come from the supposed author and the contents of the text were received exactly as sent, unless someone has learned the author's secret key and used it to forge a message digest for a message of his own or one that he has altered.

If the author wants to keep the text of the message private, so that only the intended recipient can read it, he or she can encrypt the signed message, using the recipient's public key. Then, the recipient first uses his or her own secret key to decrypt the signed message before going through the procedure described above.

---

[30] According to the vendor, the probability of two different plaintexts having the same message digest is on the order of one in a trillion.

[31] Note that for ordinary encryption to preserve privacy, the recipient's public key is the one used to encrypt.

Appendix E

Acronyms

ABA	—American Bankers Association
ACE	—American Council on Education
AICPA	—American Institute of Certified Public Accountants
AITRC	—Applied Information Technologies Research Center
ANSI	—American National Standards Institute
ATM	—Automatic Teller Machine
AT&T	—American Telephone & Telegraph Co.
BAI	—Bank Administration Institute
BJS	—Bureau of Justice Statistics
CBC	—Cipher Block Chaining
CCEP	—Commercial Communications Endorsement Program
CFB	—Cipher Feedback
CHIPS	—Clearing House Interbank Payments System
CIA	—Central Intelligence Agency
COMSEC	—Communications Security
DCA	—Defense Communications Agency
DCTN	—Defense Commercial Telecommunications Network
DES	—Data Encryption Standard
DIS	—Defense Investigative Service
DoD	—Department of Defense
DSA	—Decimal Shift and Add [Algorithm]
DTS	—Digital Termination System
EAR	—Export Administration Regulations
EBDI	—Electronic Business Data Interchange
EDI	—Electronic Data Interchange
EDP	—Electronic Data Processing
EFT	—Electronic Fund Transfer
EIA	—Electronic Industries Association
ESVN	—Executive Secure Voice Network
FBI	—Federal Bureau of Investigations
FCC	—Federal Communications Commission
FIPS	—Federal Information Processing Standards
FTS	—Federal Telecommunications Service
GAO	—Government Accounting Office
GSA	—General Services Administration
HBO	—Home Box Office
ICST	—Institute for Computer Sciences and Technology
IEEE	—Institute of Electrical and Electronics Engineers
ISDN	—Integrated Services Digital Network
ISO	—International Organization for Standardization
ISSA	—Information Systems Security Association
ITAR	—International Traffic in Arms Regulation
LAN	—Local Area Network
LSI	—Large Scale Integration
MAC	—Message Authentication
MAN	—Metropolitan Area Network
NASA	—National Aeronautics and Space Administration
NBS	—National Bureau of Standards
NCSC	—National Computer Security Center
NSA	—National Security Agency
NSC	—National Security Council
NSDD	—National Security Decision Directive
NSF	—National Science Foundation
NTIA	—National Telecommunications and Information Administration
NTISSC	—National Telecommunications and Information Systems Steering Committee
OMC	—Office of Munitions Control
OSI	—Open System Interconnection
OTA	—Office of Technology Assessment
PC	—Personal Computer
PIN	—Personal Identification Number
SDNS	—Secure Data Network System
STU-III	—Secure Telephone Unit III
S.W.I.F.T.	—Society for Worldwide Interbank Financial Telecommunications
TDCC	—Transportation Data Coordinating Committee
UCS	—Uniform Communication Standard
VLSI	—Very Large Scale Integrated Circuits
WINS	—Warehouse Information Network Standards

Appendix F

Contributors and Reviewers

CONTRIBUTORS

Kenneth Allen
David Peyton
Information Industry Association

Peter S. Brown
Profile Analysis Corp.

Thomas R. Burke
Chief, Technical Services
General Services Administration

Lawrence D. Dietz
The Alec Group

Robert C. Elander
Nancy Floyd
Citicorp/Quadstar

George F. Flynn, Jr.
Director, Special Programs Division
General Services Administration

Cathi Kachurik
Director, X3 Secretariat
CBEMA

Eleanor Kask
Time Life Books

Lisa Kuuttila
Stanford University
Office of Technology Licensing

Christine Martin
Atalla Corp.

G.T. McCoy
NASA Headquarters
Office of the General Counsel

Terri McGuire
Frost & Sullivan, Inc.

Glenn McLaughlin
Congressional Research Service
Library of Congress

Charles Miller
Director of Public Affairs
AT&T

Donn B. Parker
Senior Management Consultant
SRI International

Stuart Personick
Bell Communications Research

Jeremy Ross
Time Life Books

Joseph Smaldone
Chief, Licensing Division
Office of Munitions Control
Department of State

Jon P. Stairs
Director, Electronic Services
Information Resources Management Service
General Services Administration

Michael Thompson
Security Magazine
Cahners Publishing Co.

Denise Ulmer
Chemical Bank

Marjolijn Van der Velde
Bank Administration Institute

Steven Weiland
Bank Administration Institute

Florence Young
Advisor
Board of Governors of the Federal Reserve System
Division of Federal Reserve Bank Operations

EXTERNAL REVIEWERS

Lara H. Baker*
Los Alamos National Laboratory

Jim Bidzos
RSA Data Security, Inc.

Dennis Branstad
National Bureau of Standards

Randolph W. Bricker, Jr.
Principal
Booz-Allen & Hamilton, Inc.

Richard Case
AFIPS

David Chaum
Centre for Mathematics & Computer Science

Morey J. Chick
Manager
U.S. General Accounting Office

John Clement
AFIPS

Michael Corby
AFIPS

Prentice Cress
General Services Administration

Harold E. Daniels, Jr.
NSA

Cipher A. Deavours

Jack Dennis
Assistant Director
Division of Federal Reserve Bank Operations
Board of Governors of the Federal Reserve System

Whitfield Diffie
Bell Northern Research

---

*Retired. Replaced by Lawrence Wills.
**Ex-officio.

Jim Dray
Digital Equipment Corp.

Martin Ferris
Program Analyst
U.S. Treasury

Diane Fountaine
Mark Frankel
AAAS

Henry Geller
Consultant

Steven Gould
AAAS

Edward Hall
American Bankers Association

Martin Hellman
Stanford University

Cheryl W. Helsing
Vice President
Bank of America

Robert Jueneman
Computer Science Corp.

David Kahn
Consultant

Stuart W. Katzke
Chief, System Components Division
National Bureau of Standards

Ron Keelan
Data Security Program
IBM Corp.

Richard Kemmerer
AFIPS

Robert F. Kempf
NASA Headquarters
Associate General Counsel for Intellectual Property Law

Stanley Kurzban
IBM Corp.

Donald C. Latham
Assistant Secretary for Command, Control, Communications and Intelligence
Department of Defense

Paul Lemme
Transportation Data Coordinating Committee

Robert Massey (Retired)
National Telecommunciations and Information Administration, and Army Intelligence & Security Command

Vincent McLellan
InfoWeek

Robert Meadows
American Bankers Association

Charles Miller
Director of Public Affairs
AT&T

William Murray
Consultant

David B. Newman, Jr.
George Washington University

Robert Park
American Physical Society

David Peyton
Information Industry Association

Jon Postel
AFIPS

Charles A. Pulfrey
Director, Program Development
Unisys

Harold Relyea
Government Division
Congressional Research Service
Library of Congress

John M. Richardson
IEEE CCIP

Ron Rivest
MIT Laboratory for Computer Science

Peter Schweitzer
Consultant

Heinz Seipel
Science Counselor
Embassy of the Federal Republic of Germany

Miles Smid
National Bureau of Standards

Edward Springer
OMB OIRA

Dennis Steinauer
NBS

Rein Turn
AFIPS

Mitchel B. Wallerstein
Associate Executive Director
Office of International Affairs
NAS

Eddie L. Zeitler
Vice President
Security Pacific National Bank
Information Systems Security Division

CONTRACTORS

Bell Communications Research:
- E[illegible]t Brickell
- Daniel Collins
- Daniel Hochvert
- Kenneth Hopper
- R.J. Keevers
- Bruce Leary
- Stewart Personick
- Philip Porter
- Marc Schare
- Howard Stearns
- Richard Wolff

Ernst & Whinney:
- Robert Linnemanstons
- Catherine Travis
- David R. Wilson

Information Security, Inc.:
- Noel Matchett

Personal Identification News:
- Benjamin L. Miller

Ross Engineering, Inc.:
- James A. Ross

Consultant:
- Peter Schweitzer

OTA STAFF REVIEWERS

Michael Callaham
International Security and
Commerce Program

Vary Coates
Communication and Information
Technologies Program

Priscilla Regan
Communication and Information
Technologies Program

Fred Wood
Communication and Information
Technologies Program

Superintendent of Documents Publication Order Form

Order Processing Code
6327

Charge your order.
It's easy!

☐ **YES,** please send me the following indicated publications:

Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information.
GPO stock number 052-003-01083-6; price $8.50.

1. The total cost of my order is $_______ (International customers please add an additional 25%.) All prices include regular domestic postage and handling and are good through 1/88. After this date, please call Order and Information Desk at 202-783-3238 to verify prices.

Please Type or Print

2. ____________________
(Company or personal name)

____
(Additional address/attention line)

____
(Street address)

____
(City, State, ZIP Code)

(_______)_______________
(Daytime phone including area code)

3. **Please choose method of payment:**

☐ Check payable to the Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐☐-☐

☐ VISA, CHOICE or MasterCard Account

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

____
(Credit card expiration date)

Thank you for your order!

____
(Signature)

10/87

4. **Mail To:** Superintendent of Documents, Government Printing Office, Washington, D.C. 20402-9325

Office of Technology Assessment

The Office of Technology Assessment (OTA) was created in 1972 as an analytical arm of Congress. OTA's basic function is to help legislative policymakers anticipate and plan for the consequences of technological changes and to examine the many ways, expected and unexpected, in which technology affects people's lives. The assessment of technology calls for exploration of the physical, biological, economic, social, and political impacts that can result from applications of scientific knowledge. OTA provides Congress with independent and timely information about the potential effects—both beneficial and harmful—of technological applications.

Requests for studies are made by chairmen of standing committees of the House of Representatives or Senate; by the Technology Assessment Board, the governing body of OTA; or by the Director of OTA in consultation with the Board.

The Technology Assessment Board is composed of six members of the House, six members of the Senate, and the OTA Director, who is a non-voting member.

OTA has studies under way in nine program areas: energy and materials; industry, technology, and employment; international security and commerce; biological applications; food and renewable resources; health; communication and information technologies; oceans and environment; and science, education, and transportation.